Haachtsesteenweg 1442
1130 Brussels
Belgium

DEP Documentation

DEP PC-AUX Program User Manual

Version Management Report

Version	Name(s)	Date	Comments
01.00	TheSteamFactory	24/04/2000	First Draft
01.01	TheSteamFactory	25/07/2000	Final Draft
01.02	F. Demaertelaere	27/09/2000	Small modifications
02.00	F. Demaertelaere	12/01/2001	Final version
03.00	H. Colbrant	25/07/2002	Type DX3 added, GUI modified
03.01	F. Demaertelaere	26/02/2003	After crash
03.02	H. Colbrant	07/04/2003	Check value for each type of key
03.03	H. Colbrant	05/08/2003	Three CV available for each type of key
03.04	F. Demaertelaere	11/03/2003	Small updates
03.05	P. De Man	28/09/2005	Small updates
03.06	I. de Aguirre	02/02/2006	Update for Version 3.3.3
03.07	L. Ernes	26/06/2008	Update for Version 4.0.1 (FIPS bit, and AES key type)
03.08	C. Meuter	18/03/09	Update v4.0.2 (FIPS SSH Intro)
04.00	Anna Papayan	01.03.2011	Change the template into Atos Worldline, minor changes.
04.01	Anna Papayan	16.05.2012	Update for Version 4.2.0 (BDE configuration, support for Windows 7), Installation procedure update.

1. TABLE OF CONTENTS

2. SCOPE OF THE DOCUMENT

This document describes the *DEP PC-AUX Program*. This auxiliary program is used by the Security Officers responsible for creating or altering Definition Lists.

The document does not explain when Definition Lists have to be created or the values to enter. This information can be found in the *DEP Atos Worldline' Security Officer's Guide* or the *DEP Customer's Security Officer's Guide*.

2.1. REFERENCES

This document contains references to other documents about the DEP. This paragraph gives a list of all the documents referred to.

- *DEP Atos Worldline' Security Officer's Guide*
- *DEP Customer's Security Officer's Guide*
- *DEP C-ZAM/DEP User Manual*
- *DEP Key Backup Conversion Guide*
- *DEP Secret Sharing Mechanism*
- *DEP Key Entry Guide*

There are no references made to the following documents, but they could be useful to understand this document.

- *DEP Introduction to DEP*
- *DEP General Architecture*
- *DEP Glossary*

2.2. CONTACTING ATOS WORLDLINE

You can visit *Atos Worldline* on the World Wide Web to find out about new products and about various other fields of interest.
URL: www.atosworldline.com.

For the documentation visit the http://www.banksys.com web page.

For support on issues related to DEP, customers, partners, resellers, and distributors can send an email to the DEP Hotline:
mailto:dephotline-atosworldline@atosorigin.com.

3. PURPOSE OF DEP PC-AUX PROGRAM

The *C-ZAM/DEP* allows making operations on keys and capabilities, such as creating keys in the *C-ZAM/DEP*, saving key parts or keys on DCC's by using a defined secret sharing mechanism, … (see *DEP C-ZAM/DEP User Manual* for more information). The *C-ZAM/DEP* needs a Definition List that describes the properties of every key and/or capability for all these operations. Briefly, Definition Lists are used in the *C-ZAM/DEP* for key and capability management.

Three types of Definition Lists exist:

- Key Definition List
- Capability Definition List
- Secret Sharing Definition List

Key Definition List contains the properties of keys that are used in a specific DEP environment. Capability Definition List contains the properties of capabilities. How these keys and capabilities are divided before storage on DCC is defined in Secret Sharing Definition List.

With the *DEP PC-AUX Program* it is easy to create and/or edit Definition Lists using a PC. Once created or edited, the Definition Lists can be sent to a *C-ZAM/DEP* (and additionally be saved on DCC).

It is also possible to read the Definition Lists available in a *C-ZAM/DEP* in the *DEP PC-AUX Program* for editing or backup purpose.

Which definitions must be written into which list can be found in the *DEP Atos Worldline' Security Officer's Guide* or the *DEP Customer's Security Officer's Guide*.

In the version 3.0 of the *DEP PC-AUX Program*, the Definition Lists were adapted to allow choosing among three algorithms for the calculation of the unique check value level (four algorithms if we consider the first type ("01" NONE) that represents the choice of none check value).

From the version 3.2.2 the way keys are entered and the attached check values are completely separated. Until now, both were incorporated in the field *ENTRY*. Besides, the new Definition Lists integrate now three levels of check value that can be defined for the keys. And, for each level, a type of check value can be chosen among several algorithms (the same as in the version 3.0).

We modified the data in the Capability Definition List and Key Definition List delivered with Installation from the version 3.3.3.

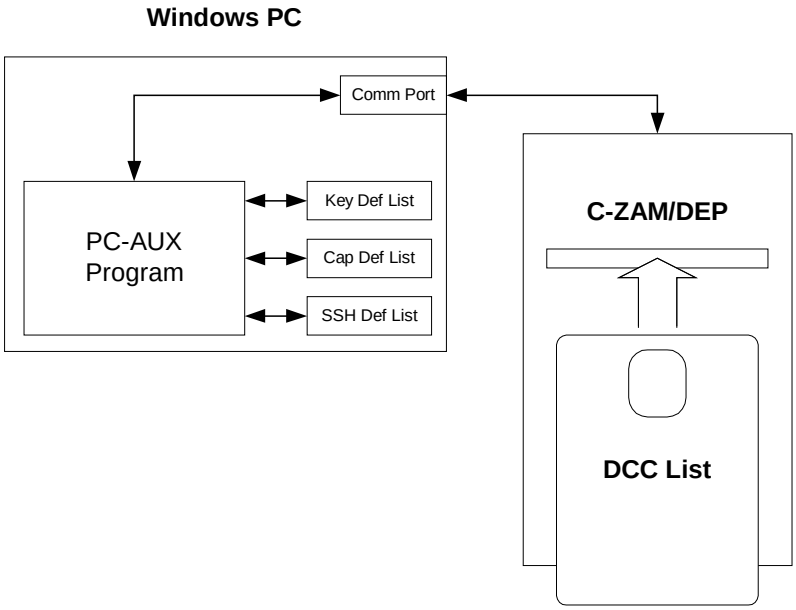
For more information about the check values' mechanisms, it is highly recommended to read the *DEP Key Entry Guide*.

4. SET-UP

4.1. HARDWARE SET-UP

The *DEP PC-AUX Program* runs on a Windows 2000, XP, Windows Vista or a Windows 7 PC.

To exchange the Definition Lists with a C-ZAM/DEP, at least one free serial communication port (COM1 or COM2) is required. The *C-ZAM/DEP* can then be connected to this communication port using a dedicated serial cable.



4.2. SOFTWARE SET-UP

The *DEP PC-AUX Program* should be installed on PC. An installation procedure for the *DEP PC-AUX Program* exists. To start the installation wizard of the *DEP PC-AUX Program*, insert first the installation CD_ROM or download it from internet and start the ***Setup.exe***.

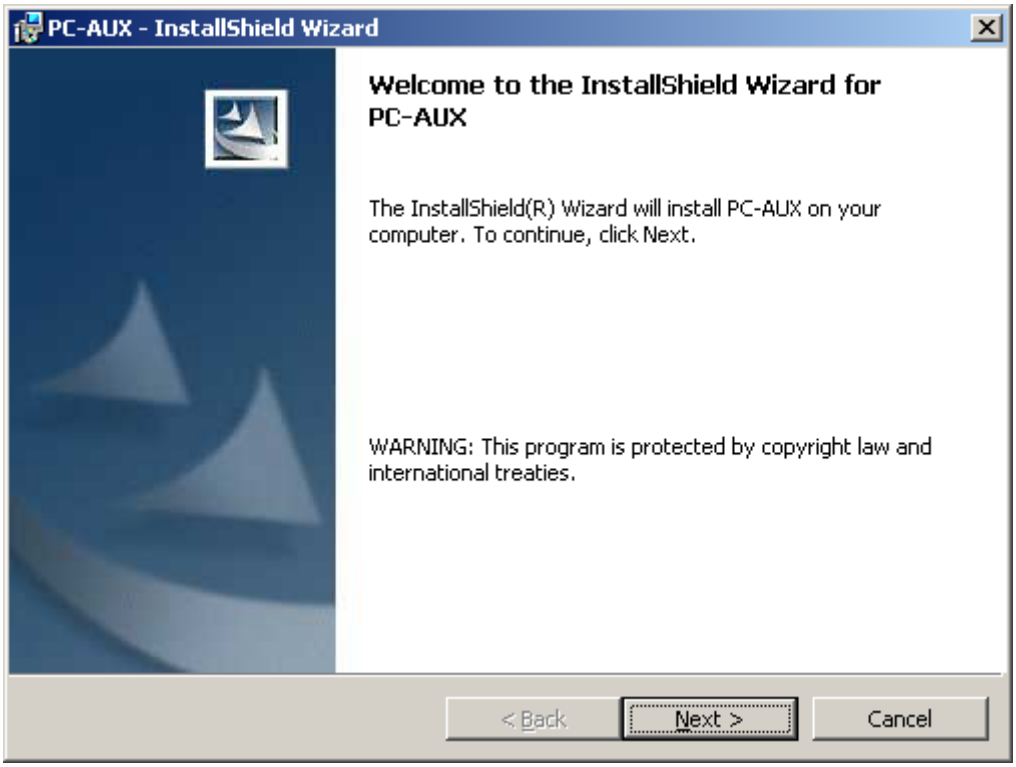
Remark that together with the *DEP PC-AUX Program*, another auxiliary program is installed, that allows the conversion of former generation of key backups to a DEP key backup (see the document *DEP Key Backup Conversion Guide*).

Note:

A user must have administrative privileges to be able to start the installation procedure.

4.2.1. Welcome

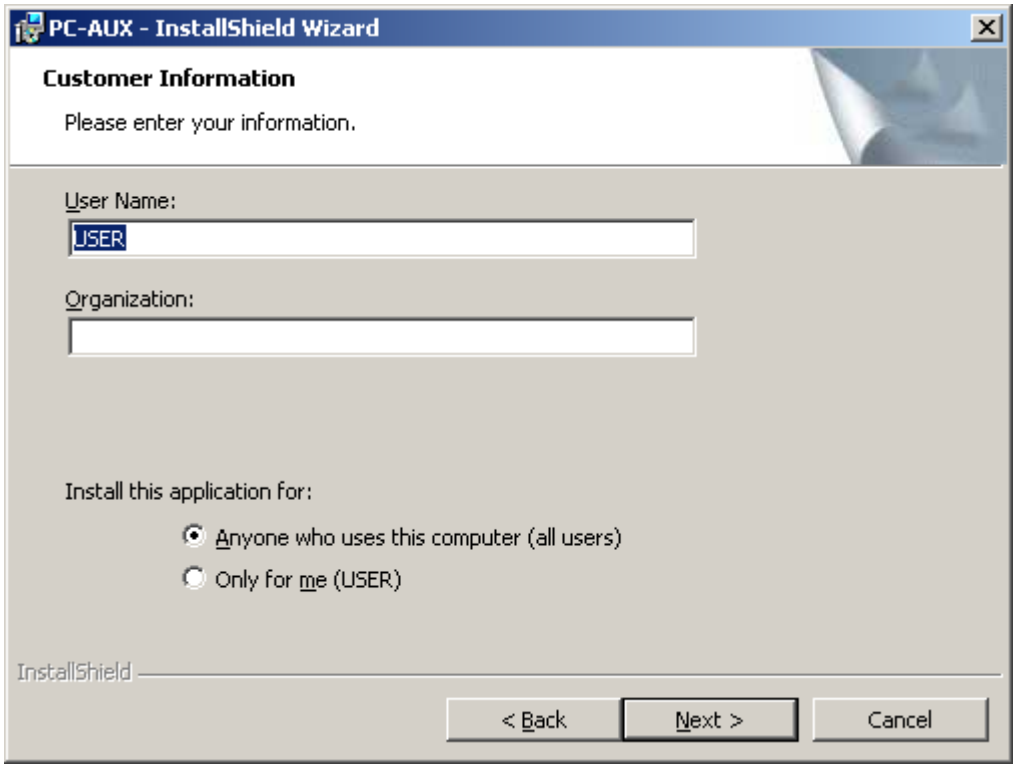
A *Welcome* screen appears immediately after the execution of the ***Setup.exe***. It contains some recommendations and warnings about the copyright laws and international treaties.



Click the *Next* button to continue the installation procedure, *Back* to return to the previous screen or *Cancel* to abort.

4.2.2. User Information

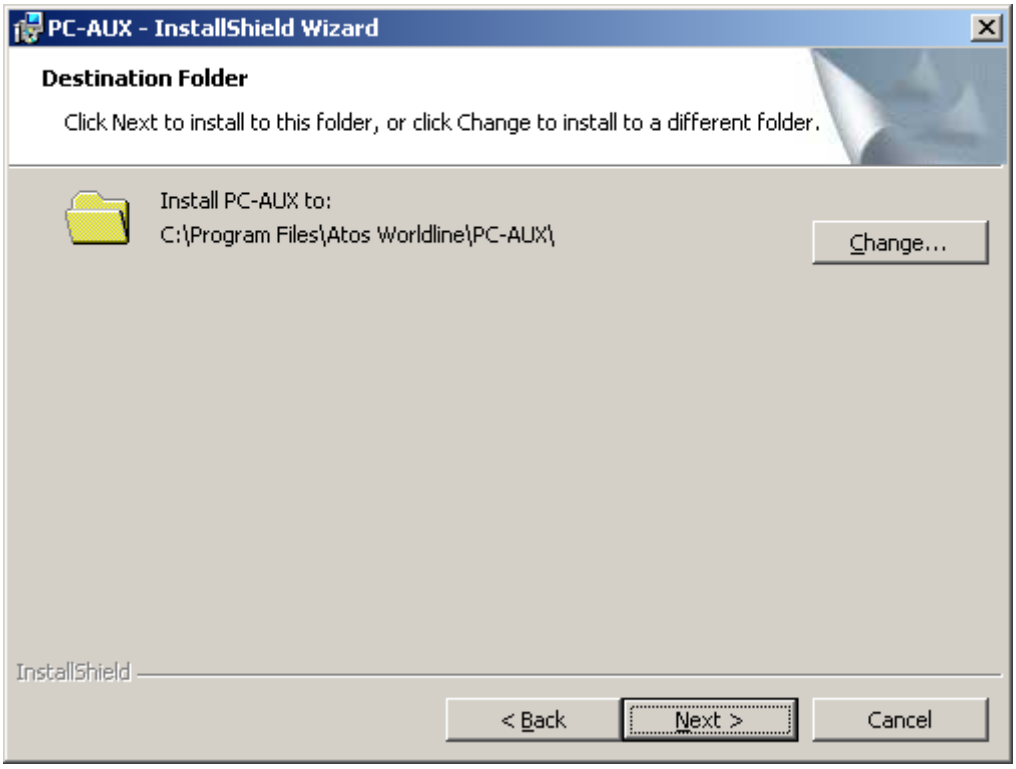
The *User Information* screen allows to enter the user name and the name of the company that performs the installation.



Enter the user and the organization names in appropriate fields, select the users group for the application and click the *Next* button to continue. Click *Back* to return to the previous screen or *Cancel* to abort the installation procedure.

4.2.3. Choose Destination Location

At the *Destination Folder* step the destination directory for the application should be selected. It defines the path where the *DEP PC-AUX Program* will be installed. The default path is **C:\Program Files\Atos Worldline\PC-AUX**.

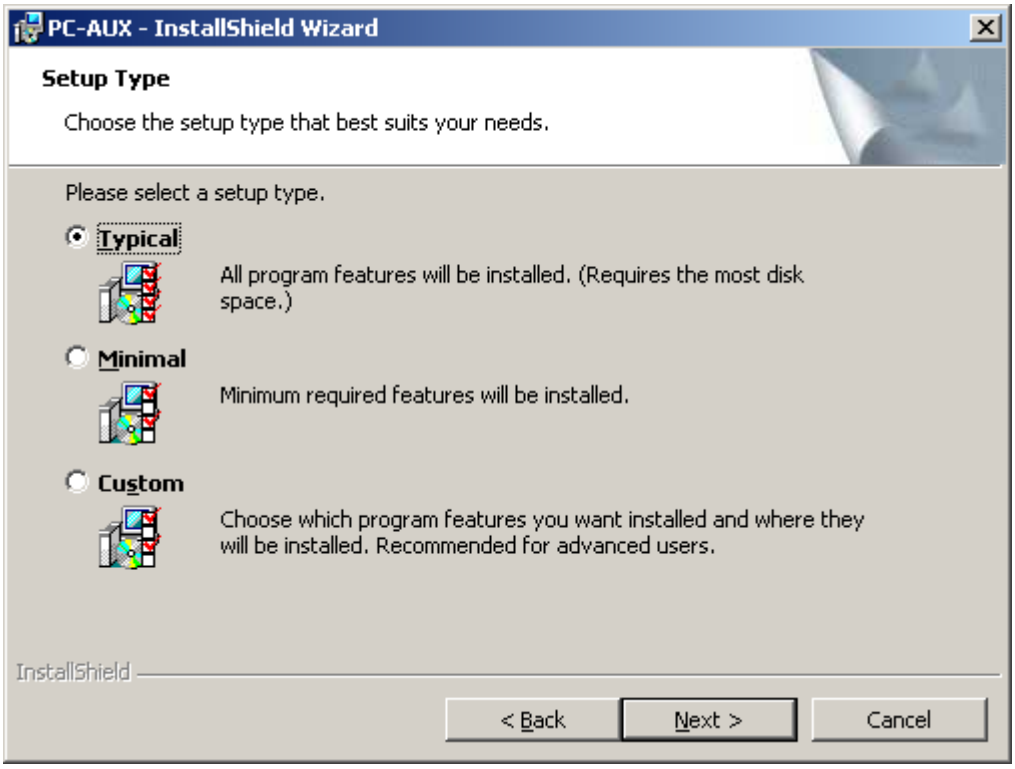


Although it is recommended to use the default path, click the *Change...* button to select another directory for the installation of the *DEP PC-AUX Program* software.

Click *Next* to continue, *Back* to return to the previous screen or *Cancel* to abort the installation procedure.

4.2.4. Choose a Setup Type

At this step the setup type for the application should be selected.

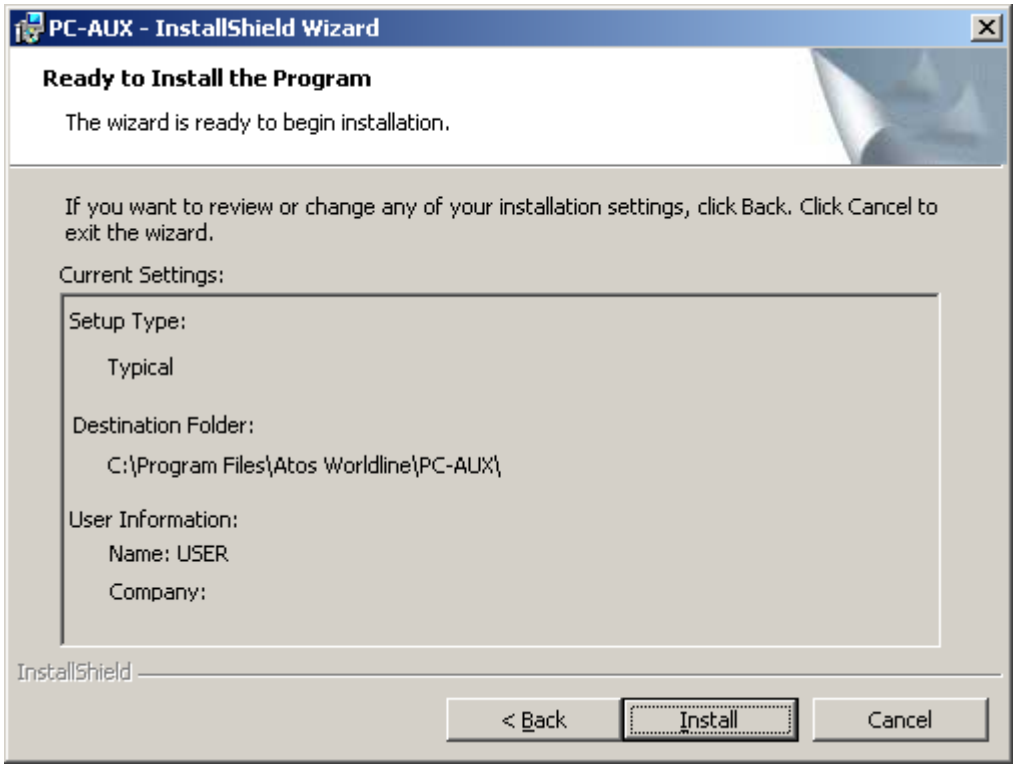


Although, it is suggested to install the **Typical** setup type, in specific cases the **Minimal** or **Custom** types can be chosen. By selecting the Typical setup type all the application features will be installed. The Minimal setup type will install the minimum required features. To install the specific program features choose the Custom type.

Click *Next* to continue, *Back* to return to the previous screen or *Cancel* to abort the installation procedure.

4.2.5. Installing the Program

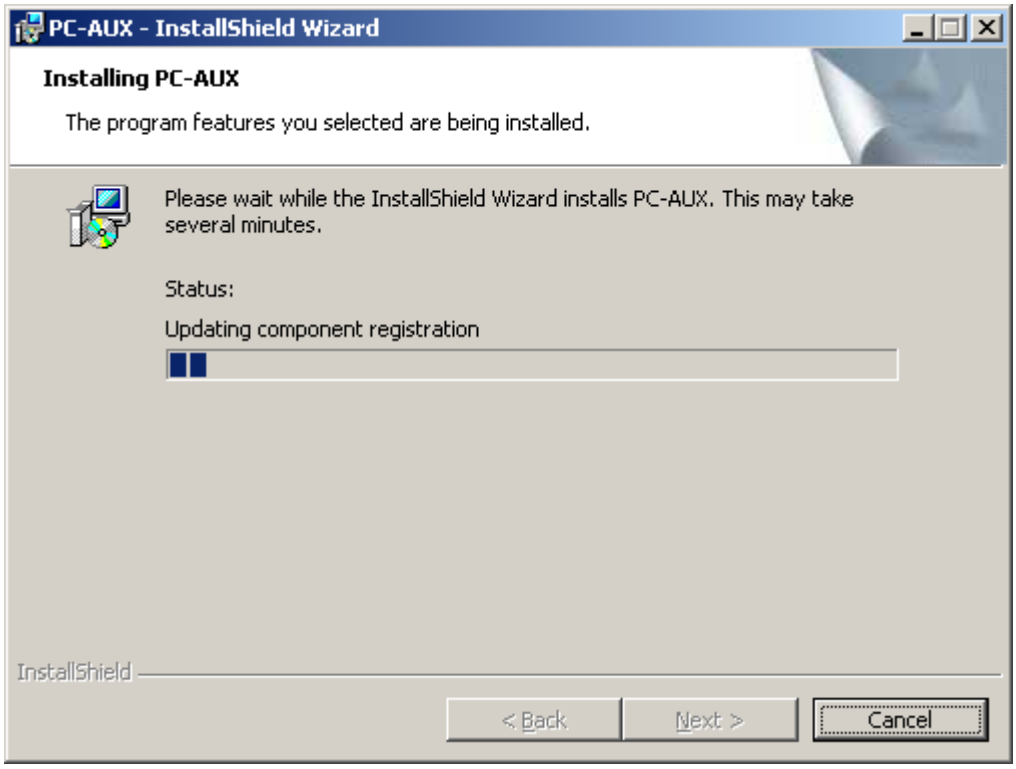
The *Ready to Install the Program* window gives an overview of the settings selected during the installation procedure.



When the information is correct, click the *Next* button to continue, go *Back* to modify some settings or use *Cancel* to abort the installation procedure.

4.2.6. Installing…

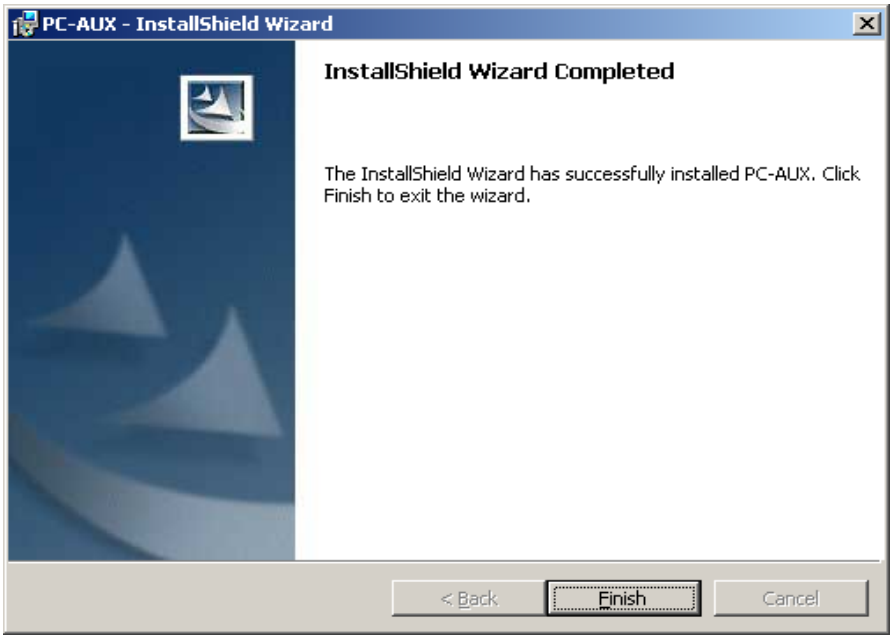
After clicking the Next button of the *Ready to Install the Program* window, all the required installations will be executed. The following window will be opened.



A progress bar and one or more status messages appears during the installation of the files.

4.2.7. Setup Complete

When all the files and information are copied, an *InstallShield Wizard Completed* window appears to confirm a successful installation.



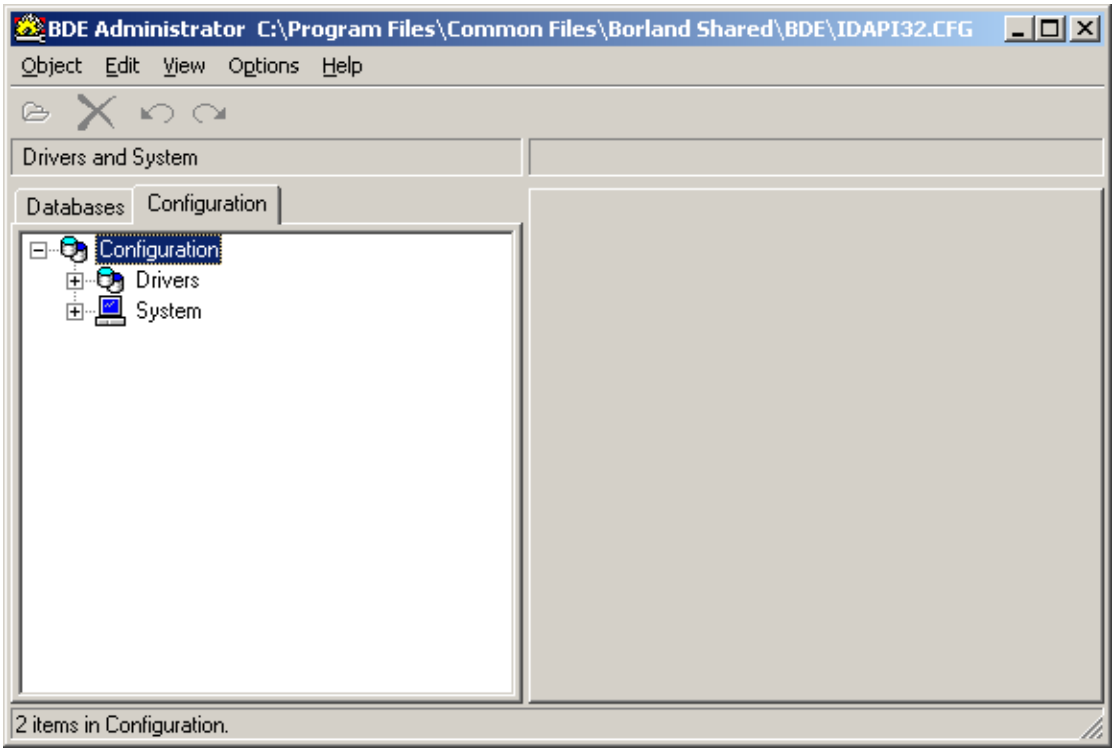
Click *Finish* to confirm the message.

4.2.8. Post Installation Steps

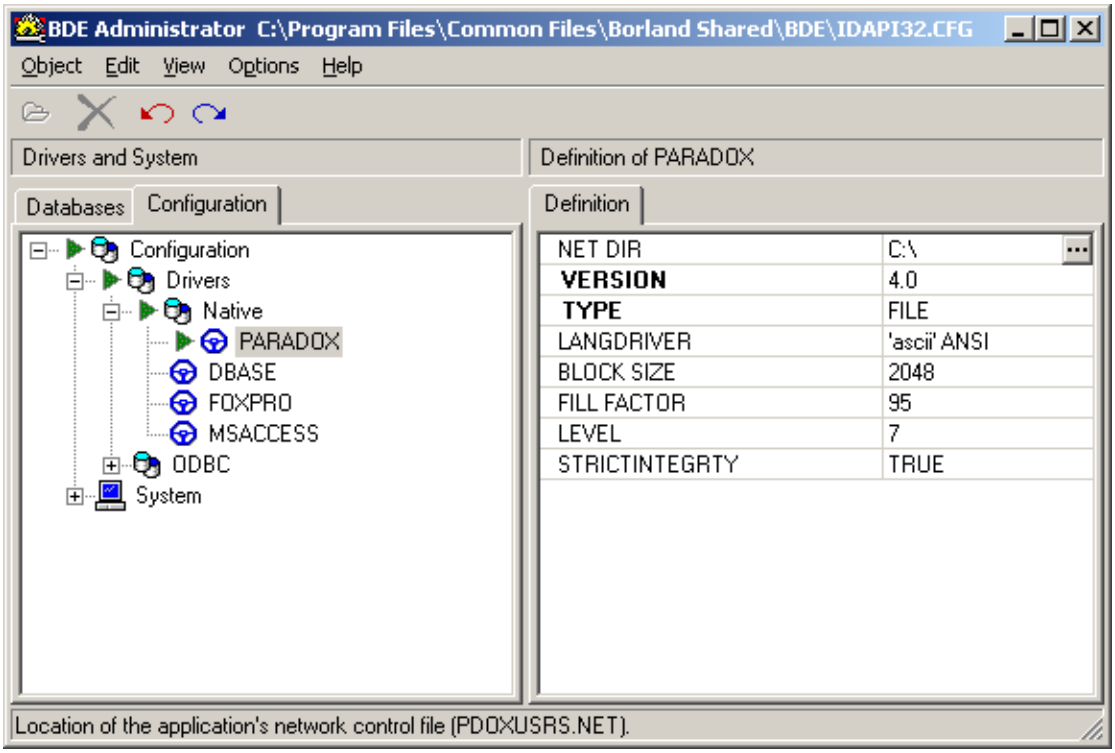
4.2.8.1.Configure Borland Database Engine

After installing the PC-AUX, the following configuration should be done in Borland Database Engine.

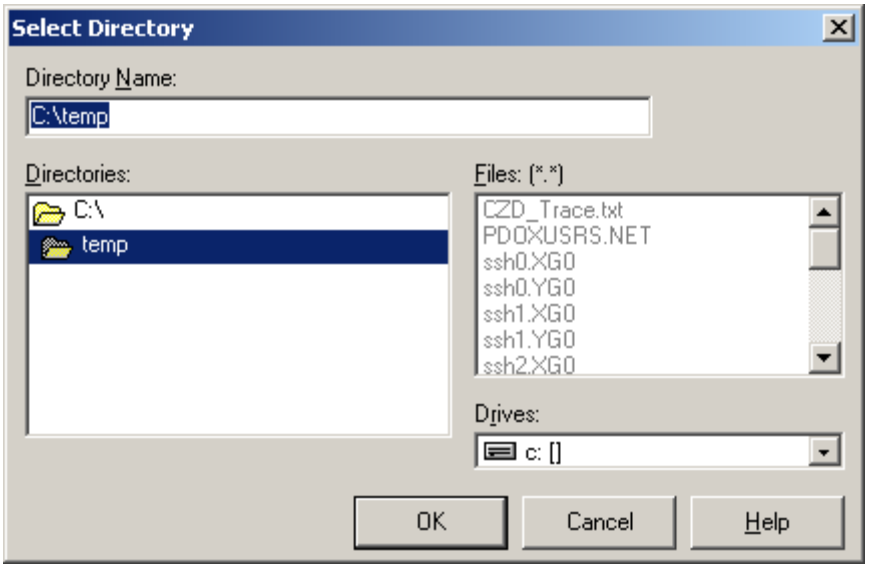
In Control Panel open the DBE Administrator program. Following window will be opened.



Open the *Drivers* item and select the **PARADOX** from the *Native* submenu.



Select the *NET DIR* property in the *Definition* panel and change the directory to **C:\temp**.



Be aware that this configuration should be done by all users on PC, otherwise it will be saved only for an Administrator user.

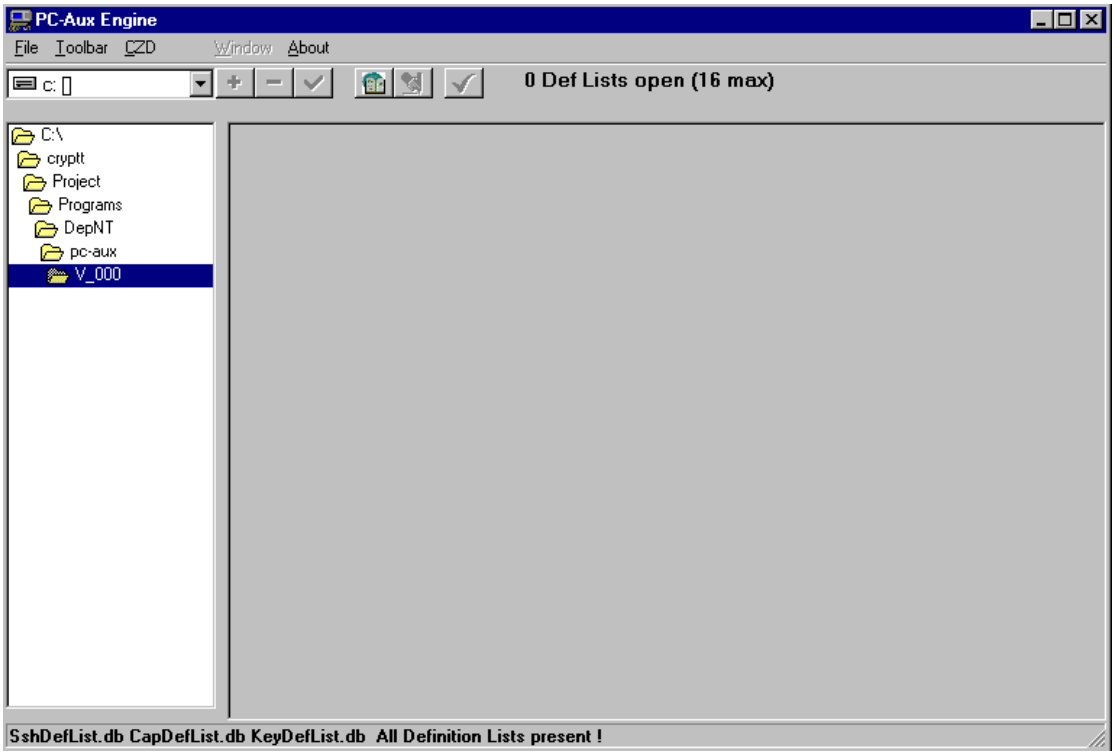
5. USER INTERFACE

5.1. START-UP WINDOW

Once the *DEP PC-AUX Program* is started, a dedicated *PC-Aux Engine* window is opened.

The main window's components are:

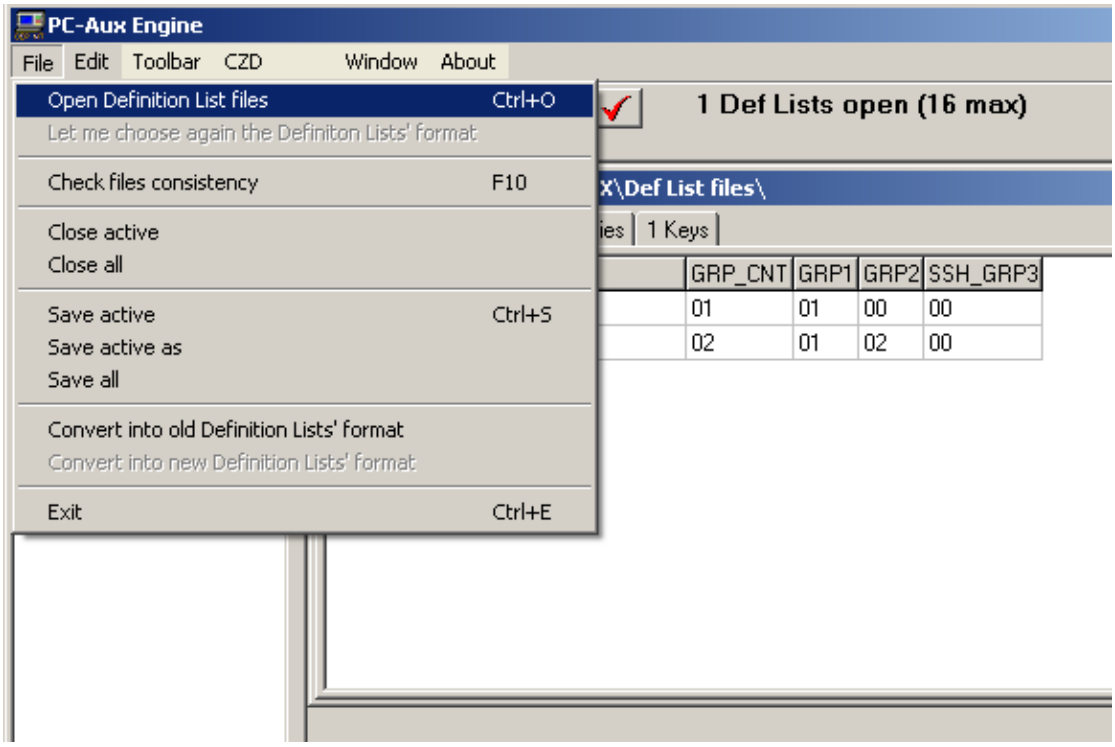
- a menu
- a dropdown box with the possible drives
- an explorer panel that will be used to select the Definition List files
- an empty panel (close to the explorer) that will contain the open Definitions List files
- a status bar
- a toolbar



5.2. FILE MENU

During the *DEP PC-AUX Program* installation, a set of Definition List files was installed in the installation directory's sub-folder *Def List files*. Use these files as a template to make your own Definition List files from scratch.

It is also possible to open existing Definition Lists and edit them according to the necessary requirements.



5.2.1. Open Definition List files

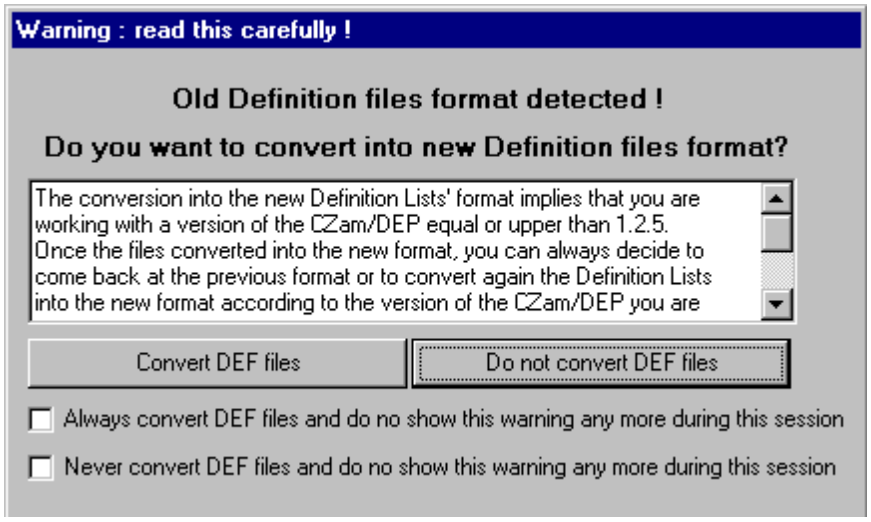
Opening a set of Definition List files means that three database files must be opened:

- *KeyDefList.db*
- *CapDefList.db*
- *SshDefList.db*

When the application starts up, the selected folder is the installation folder. So, if you want to open the Definition List files installed in the *Def List files* sub-folder, double-click on this folder and notice that the status bar indicates that the three Definition List files (the database files but also, implicitly, the index files) are present in the selected folder. It means that you are allowed to open them. To perform this operation, use the **Open Definition List files** menu item.

More generally, use the explorer to select any folder by double-clicking the directory containing the Definition List files you want to open. For each selected folder, the status bar always indicates which Definition List files are present and reacts by enabling or by disabling the **Open Definition Lists files** menu item.

Although the Definition List's format changed from version 3.2.2, the former Definition List files that defined the keys are although still usable, whichever version you are working with (3.0 or higher). When old Definition Lists are being opened, a message gives the possibility for the user to convert these old lists into the new format or to keep the old format.



This message asks the user to make a choice (convert Definition List files or not). Be aware that converted Definition Lists files require a version of the *C-ZAM/DEP* equal or upper than 1.2.05.

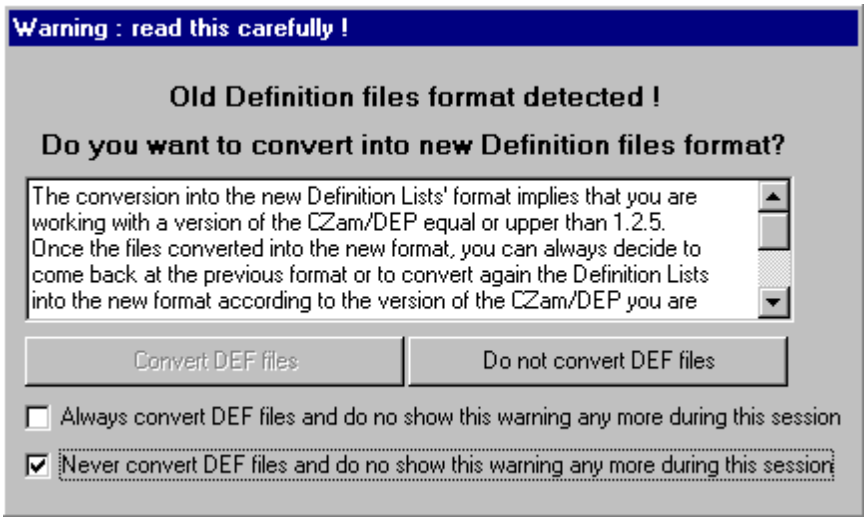
But even if the Definition Lists files were converted into the new format, they can again be reconverted into the old format and so run with a version of the *C-ZAM/DEP* lower than 1.2.05.

In case of Definition Lists already converted, the warning is not displayed.

Two options are available:

- Always convert DEF files and do not show this warning anymore during this session
- Never convert DEF files and do not show this warning anymore during this session

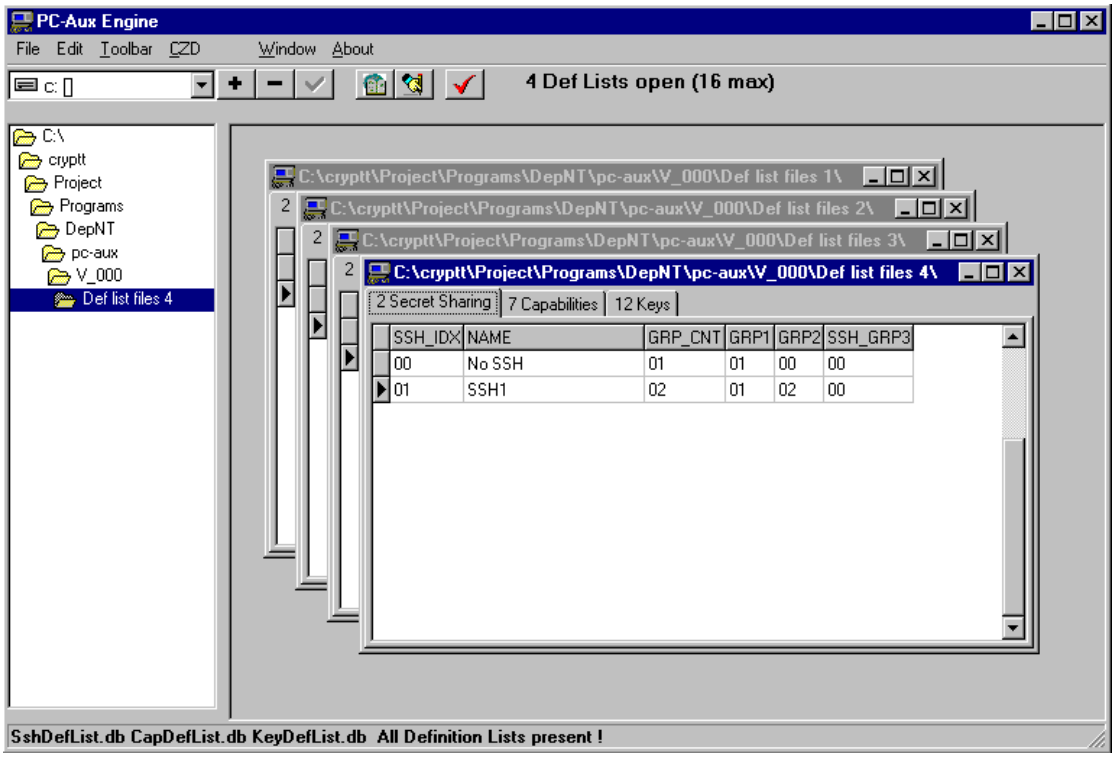
If one of these options is checked, the warning message will no more be shown, except if the user mentions it explicitly (see paragraph 5.2.2 on page 20). In the example here below, the user has chosen that the Definition Lists will never be converted.



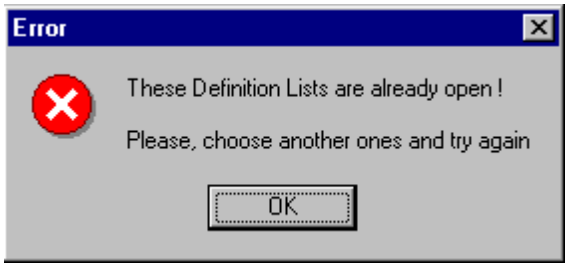
For more information about the conversion, see paragraphs 5.2.9 and 5.2.10 on page 24.

After opening, the Definition List files appear in a new sub-window in the panel close to the explorer. In this sub-window, three tabs *Secret sharing*, *Capabilities* and *Keys* contain the Definitions List files' records.

A maximum of 16 sets of Definition List files can be open in parallel.



It is not allowed to open a set of Definition List files twice. The following error message appears when an already opened Definition List is tried to be opened again.



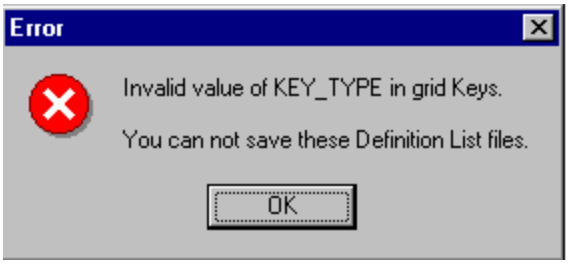
5.2.2. Let me choose again the Definition Lists' format

The **Let me choose again the Definition Lists' format** menu item is enabled when the user has checked an option in the window asking if the Definition Lists are always or never converted (see paragraph 5.2.1 on page 17).

By clicking on this menu item, the selection is cleared. During the opening of the next old Definition Lists files, the message asking if the files must be converted or not will be shown again.

5.2.3. Check files consistency

The **Check files consistency** menu item checks the integrity of the Definition Lists. It verifies that the encoded information is valid as described in paragraph 6 on page 38 and shows an error if it is not the case.



For example the values introduced in the *SSH_IDX* field of the *Capabilities* and *Keys* tabs must be defined in the *Secret Sharing* tab, where the SSH_IDX field identifies each Secret Sharing (see paragraphs 6.3 and 6.4 on pages 39 and **Error! Bookmark not defined.**). Otherwise, an error is raised.

Remark that:

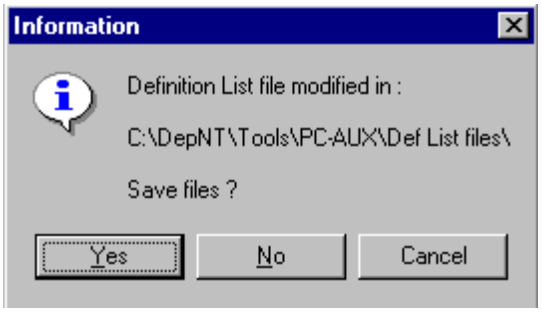
- The **Check files consistency** only verifies the active Definition List files.

Make active the sub-window for which a consistency check is required (see paragraph 5.6.3 on page 36) and select the **Check files consistency** in the **File** menu. This functionality can also be launched by clicking on the  button in the toolbar or simply pressing F10.

- When an error is detected, the application stops on the wrong record. Correct the error and launch again the **Check files consistency** to end the verification.

5.2.4. Close active

The **Close active** menu item closes the active sub-window and proposes to save its Definition List files if they have been modified but not yet saved.



Make active the sub-window that needs to be closed (see paragraph 5.6.3 on page 36) and select **Close active** in the **File** menu.

5.2.5. Close all

Where **Close active** closes only the active sub-window, the **Close all** menu item closes all the sub-windows and proposes to save their Definition List files if they have been modified and not yet saved.

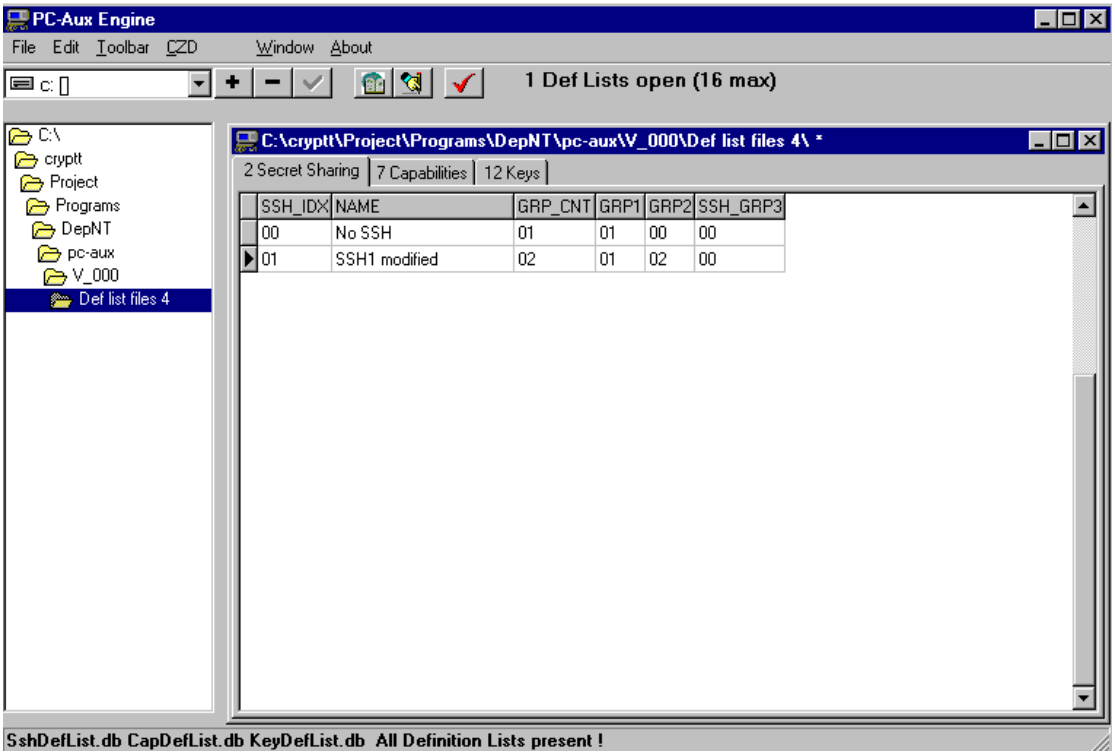
5.2.6. Save active

The **Save active** menu item is used for saving modified Definition List files or Definition List files coming from a *C-ZAM/DEP* (see paragraph 5.5.2 on page 32).

Make active the sub-window that needs to be saved (see paragraph 5.6.3 on page 36) and select **Save active** in the **File** menu.

If the sub-window was never saved (e.g. the Definition List files are coming from the *C-ZAM/DEP*), the **Save active** functionality is automatically converted to a **Save active as** (see paragraph 5.2.7 on page 22).

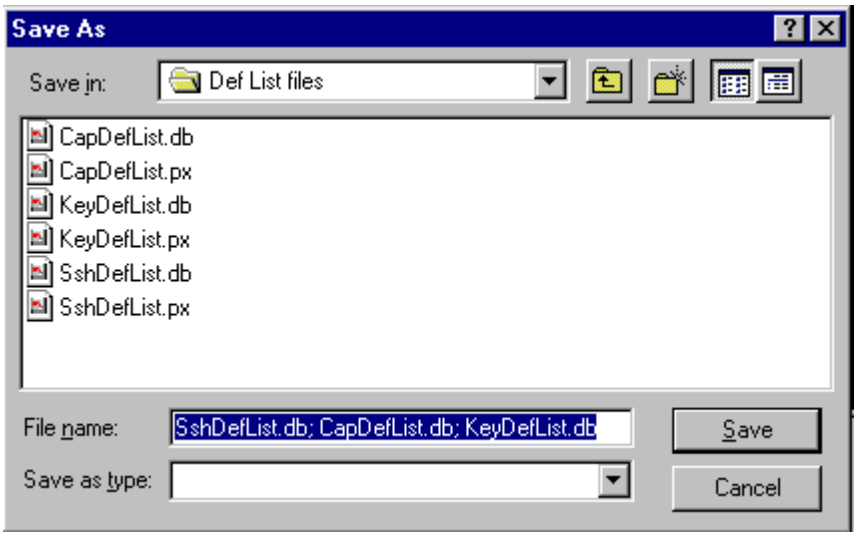
Notice that as soon as the Definition List files have been modified, a star appears in title bar of the sub-window, warning that the Definition List files need to be saved to keep the modifications.



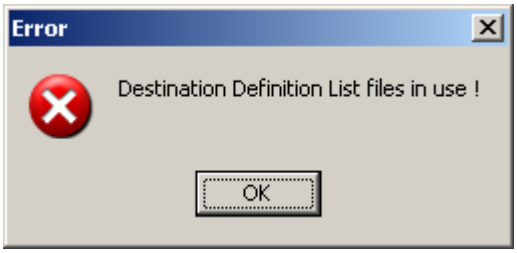
5.2.7. Save active as

As it is not possible to save the Definition List files by giving them another name, use **Save active as** to save them in another folder that contains none opened set of Definition List files.

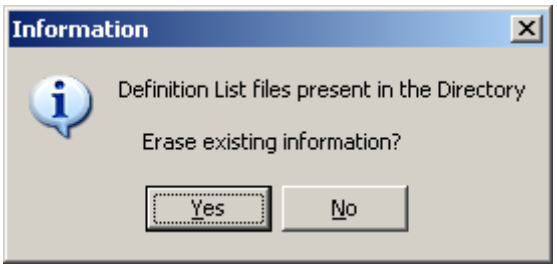
Make active the sub-window, which you want to save in another folder (see paragraph 5.6.3 on page 36) and select **Save active as** item in the **File** menu.



If the Definition List files in the destination folder are already open, an error message is received.



When Definition List files already exist (but are not open) in the destination folder, an information message asks confirmation for erasing the existing Definition List files and for replacing them by the new Definition Lists.



The **Save active** and **Save active as** functionalities include an automatic *Check files consistency* (see paragraph 5.2.2 on page 20).

Making a copy of Definition Lists or creating a template for Definition Lists are two examples for using the **Save active as** menu item.

5.2.8. Save all

The **Save active** and **Save active as** functionalities only save the active sub-window. The **Save all** menu item saves all the open Definition Files at their current location.

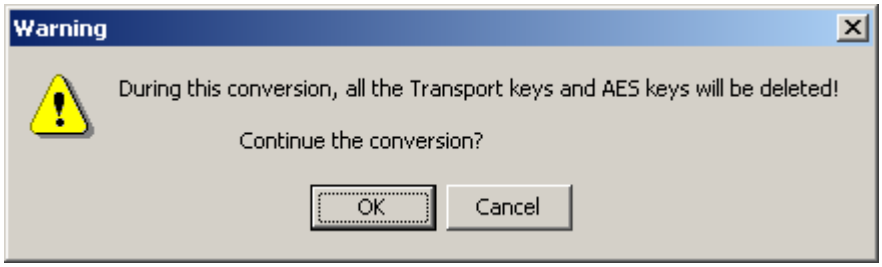
5.2.9. Convert into old Definition Lists' format

To convert the new Definition Lists into the old format select **Convert into old Definition Lists' format** menu item.

This conversion will discard unsupported features in the old format:

- the possibility to choose a check value (in columns *CV1*, *CV2*, *CV3*) for all the key definitions;
- the possibility to choose a Key Reconstruction in the DEP;
- the possibility to choose an AES key type.

NOTE: during the conversion all the transport keys and the AES keys will be deleted. A message is displayed for confirmation:



After the conversion, the trace of the previously selected check values is lost forever, as well as the information that the key has to be reconstructed in the DEP. When the Definition Lists are again converted into the new format, the key definitions will receive default values according to the explanations given in paragraph 5.2.10 on page 24.

5.2.10. Convert into new Definition Lists' format

This menu item is enabled when working with old Definition Lists. Clicking the **Convert into new Definition Lists' format** converts the Definition List into the new format.

In the field *KR*, the conversion puts the '0' value indicating the old way to reconstruct the key (i.e. in the CZAM/DEP).

In the field *CV1*, the conversion puts a value corresponding to the old format's check value. The check values at *CV2* and *CV3* are set to "01" (NONE), which means that no check value is defined for the moment. The conversion makes it possible to choose between three specific check values for each key defined in the fields *CV1*, *CV2*, *CV3*.

Moreover, the conversion gives a new identifier to the key types (see paragraph 6.4.5 on page **Error! Bookmark not defined.**) in the *ENTRY* column. A new key type replaces three old key types:

- Old **02** (FULL) type (in column **ENTRY**) remains **02** (DEF**)** type with **03** (FULL) as check value (in column CV1).
- Old **03** (NORM) type (in column **ENTRY**) becomes **02** (DEF**)** type with **02** (NORM) as check value (in column CV1).
- Old **04** (NONE) type (in column **ENTRY**) becomes **02** (DEF**)** type with **01** (NONE) as check value (in column CV1).
- Old **05** (POOL) type (in column **ENTRY**) becomes **03** (POOL**)** type with **02** (NORM) as check value (in column CV1).
- Old **06** (ENC) type (in column **ENTRY**) becomes **04** (ENC**)** type with **02** (NORM) as check value (in column CV1).
- Old **07** (XOR2) type (in column **ENTRY**) becomes **05** (XOR2**)** type with

02 (NORM) as check value (in column CV1).

- Old **08** (XOR3) type (in column **ENTRY**) becomes **06** (XOR3**)** type with **02** (NORM) as check value (in column CV1).
- Old **09** (XR2A) type (in column **ENTRY**) becomes **07** (XR2A**)** type with **02** (NORM) as check value (in column CV1).
- Old **0A** (XR3A) type (in column **ENTRY**) becomes **08** (XR3A**)** type with **02** (NORM) as check value (in column CV1).
- Old **0B** (DX3) type (in column **ENTRY**) becomes **09** (DX3**)** type with **02** (NORM) as check value (in column CV1).

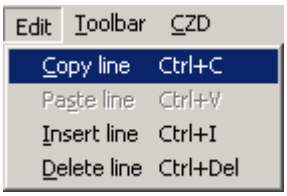
5.2.11. Exit

The **Exit** menu item is used to exit the *DEP PC-AUX Program*.

Before quitting, it verifies if all the sub-windows have been saved and proposes to save those that have been modified but not saved before really quitting the application.

5.3. EDIT MENU

The **Edit** menu allows to construct easily Definition List files and to manipulate them by inserting, copying, modifying and deleting records. All the **Edit** menu's functionalities can also be launched via the context menu.

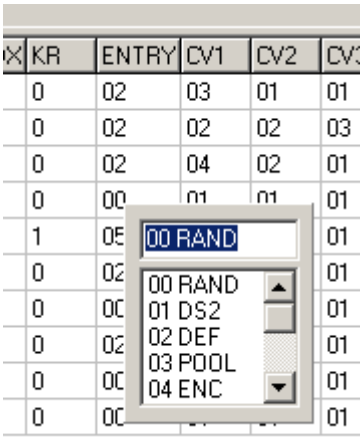


As soon as a set of Definition List files is opened, it can be edited. But before modifying it, you have to be familiar with the encoding rules defined in paragraph 6 on page 38 (see also the *DEP Key Entry Guide* document).

5.3.1. Enter Values

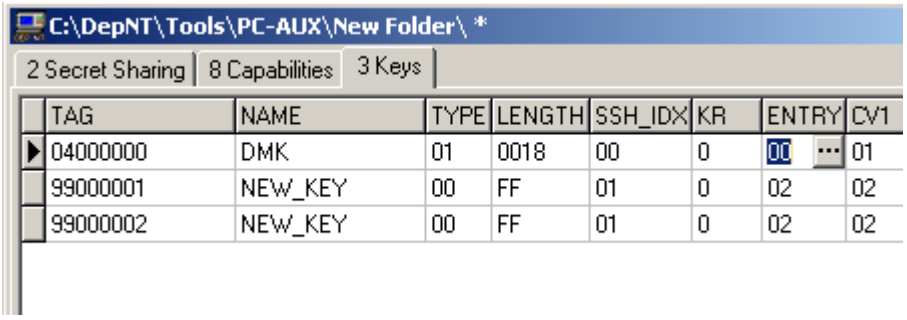
5.3.1.1.General Mechanism

For helping the user to encode the fields' values and to avoid as many as possible the encoding of wrong data, each field keeps a list with the possible values that can be introduced. Most of the lists contain static values (i.e. fixed by the application), but give additional information. For example, the list on the *ENTRY* field in the *Keys* tab indicates that the value "00 RAND" concerns a random key, "01 DS2" concerns a key coming from a DS2 backup, …



Use these lists to fill in or to modify a line by selecting the appropriate value for each field. The main steps and rules for a field modification are:

1) First select the field you want to modify and then single click on it. If values are available, the ··· button appears,



2) Click on the button ··· to make the values visible,

3) A single click on an item in the list puts the value at the top of the list as well as in the field that must be modified. At this moment, the button *POST* (see the toolbar in the previous scheme) becomes enabled. Although, the value is not yet posted in the database,

4) To validate the data, click on the *POST* or press *ENTER*: the value is now modified.

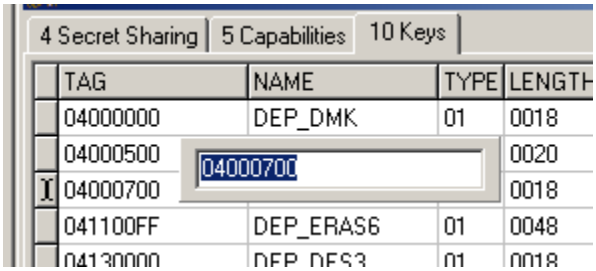
Remark that double-clicking on an item in the list immediately changes the value.

There are two reasons why no predefined values are available for a field:

- The field cannot be modified, as for *CV1*, *CV2* and *CV3* in the case of the old Definition List files or for the key entry modes “00” (RANDOM) and “01” (DS2 BACKUP).

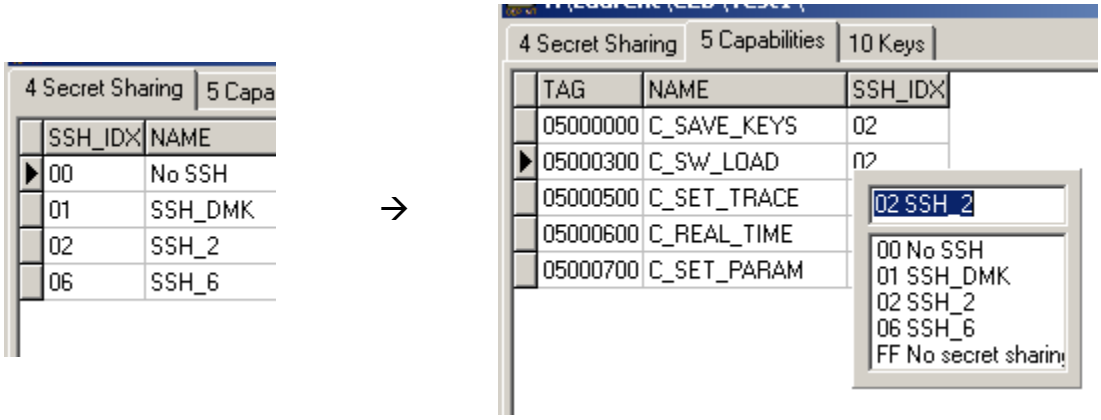
- The user can freely define the values (e.g. for the fields TAG and NAME). In this case, an edit box appears below the value to modify. Change the

value and post it with the button *POST* or by pressing ENTER. "Freely" means that, if there is not predefined values, the data must although meet a number of requirements, as for the TAG of a key (8 HEX characters beginning with "04").



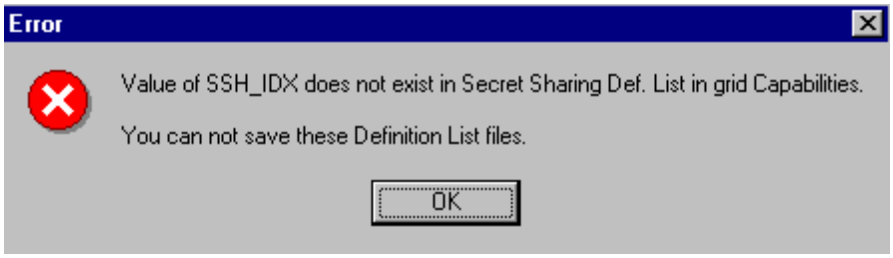
5.3.1.2. Dynamic Values

The *SSH_IDX* list in the *Capabilities* tab or *Keys* tab displays the values defined in the *Secret Sharing* tab. The *SSH_IDX* and the *SSH_NAME* fields shown in this list are pointers to the corresponding fields in the *Secret Sharing* tab.



This means that, adding or deleting a line in the *Secret Sharing* tab modifies the content of these *SSH_IDX* list.

If a field in the *Capabilities* or *Keys* still contains a deleted *SSH_IDX*, the *Check files consistency* (see paragraph 5.2.3 on page 20) will arise an error.

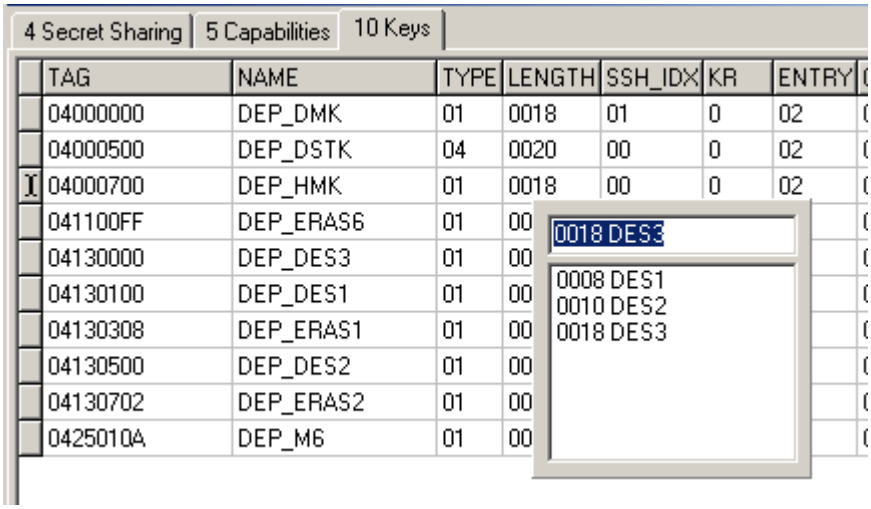


5.3.1.3. Length Values

The *LENGTH* field in the *Keys* tab combines a list in which a value can be picked or directly encoded in the upper field. The data encoded (4 characters) must be

hexadecimal values.

The proposed values in the list depend on the TYPE field. Here, for DES key:



5.3.2. Copy line

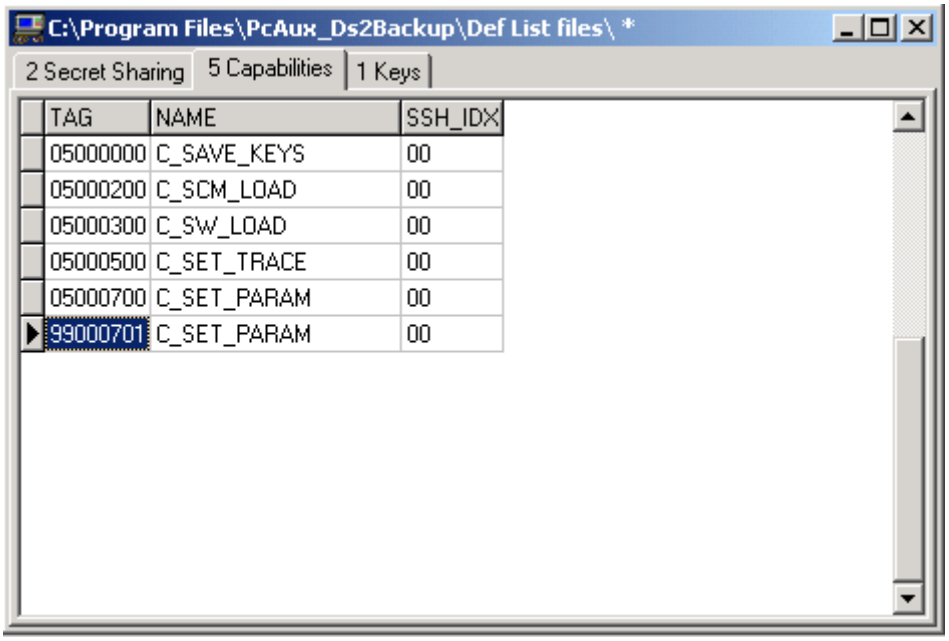
An entire line (or record) in a tab of any sub-window can be copied and pasted in same tab or in the tab of another sub-window, as far as you stay working in the same "kind" of tab (you cannot copy a line in the *Secret Sharing* tab and past it in the *Capabilities* tab).

To copy a line, click on a record and select the **Copy line** menu item from the **Edit** menu.

5.3.3. Paste line

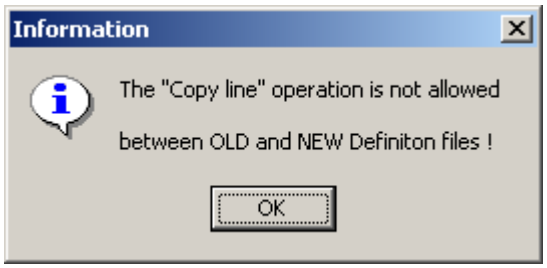
A line copied into the clipboard (see paragraph above) can be pasted into by selecting the **Paste line** menu item from the **Edit** menu.

Do not forget that the destination tab must remain in the same "kind" of tab, in the current or in another sub-window.



If the identifiers *SSH_IDX* in the *Secret Sharing* tab, *TAG* in the *Capabilities* tab and *TAG* in the *Keys* tab already exist in the tab where the line is copied, they receive a new value based on the last record 's value, increased (+ 1_{HEX}). In case of the *Capabilities* and *Keys* tabs, the two first characters of the tag are voluntarily put into a wrong value ("99") in order to avoid adding mindlessly new keys or capabilities that will be then sent uselessly into the *C-ZAM/DEP*.

But pay attention, for the *Keys* tab, a line cannot be copied between an old and a new Key Definition List. The reason is that the key types do not correspond and would introduce confusion.

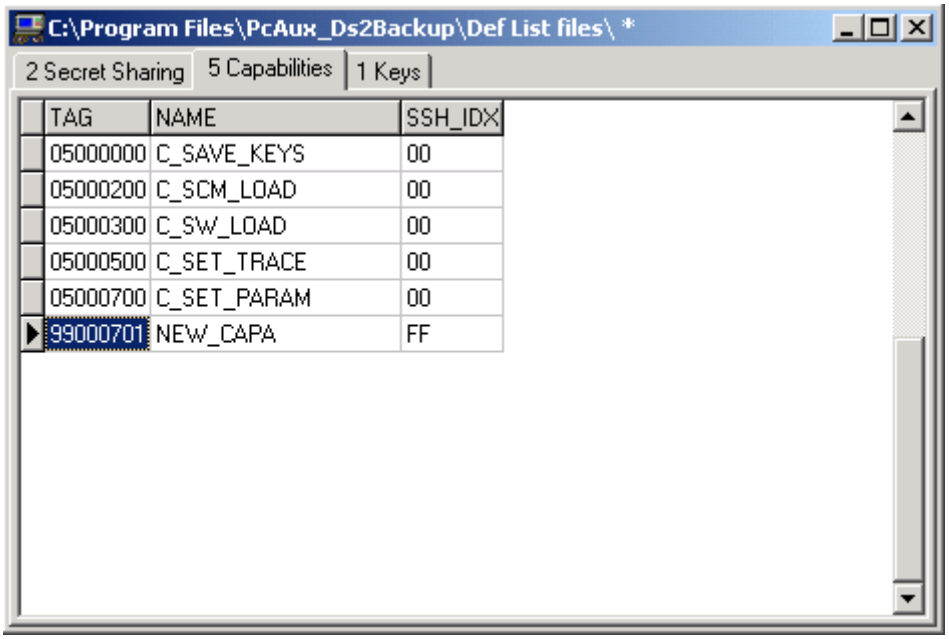


An undo function is possible by pressing the *ESC* key before the validation.

5.3.4. Insert line

The **Insert line** functionality inserts a line with default values and with identifiers for the *Capabilities* and *Keys* tabs. To construct the identifier in the key field of each record inserted, the same rules as for the copy of a line (see paragraph 5.3.3 on page 28) are followed.

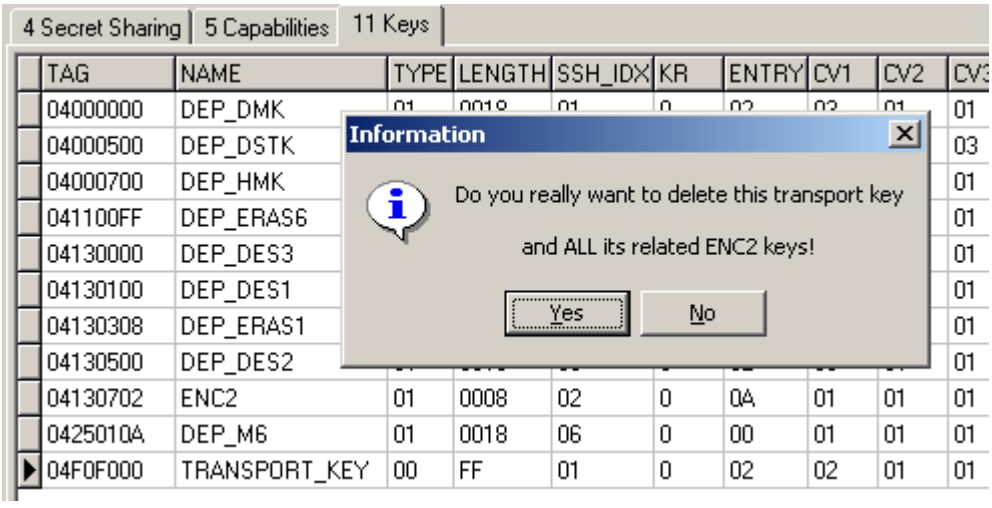
Select **Insert line** in the **Edit** menu or click the  button to insert a new line in the list



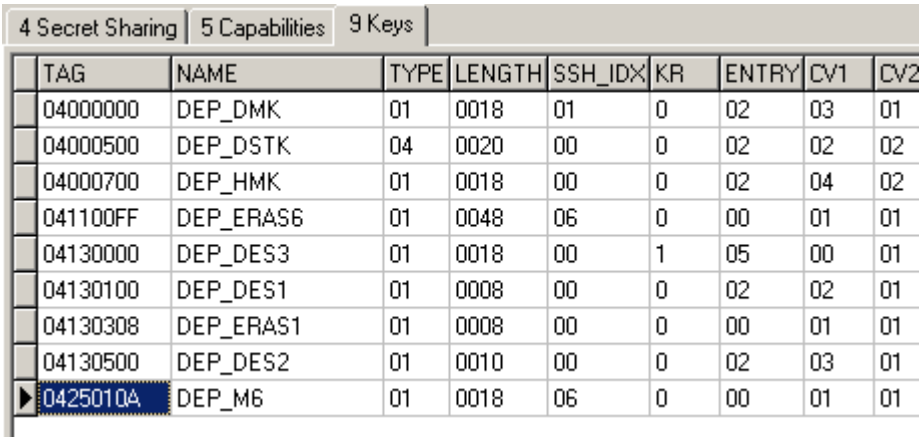
5.3.5. Delete line

Delete line is used to delete a complete line. Just select the record and click the **Delete line** menu item in the **Edit** menu. A message asks to confirm the deletion.

The deletion of a transport key causes the deletion of all its related *ENC2* keys. In the following example, the deletion of the transport key “04F0F0001” causes the deletion of the *ENC2* key “040000014”.



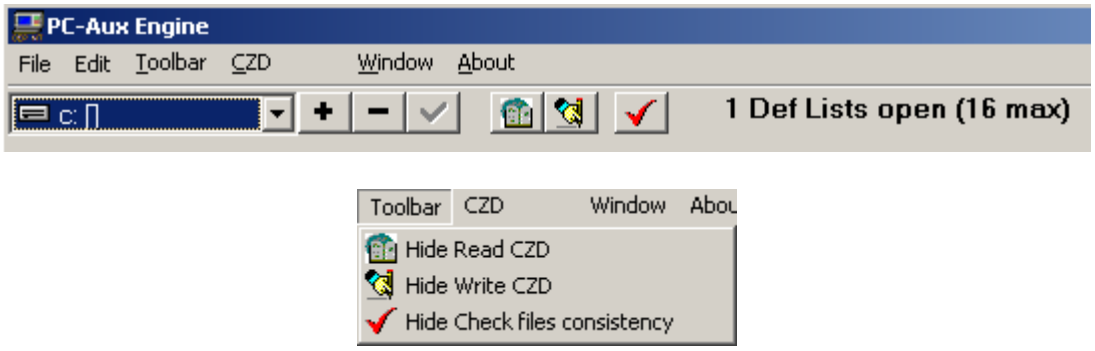
The transport key and its related *ENC2* key have been deleted:


4 Secret Sharing | 5 Capabilities | 9 Keys

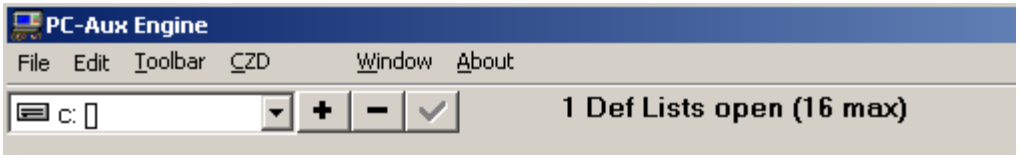
TAG	NAME	TYPE	LENGTH	SSH_IDX	KR	ENTRY	CV1	CV2
04000000	DEP_DMK	01	0018	01	0	02	03	01
04000500	DEP_DSTK	04	0020	00	0	02	02	02
04000700	DEP_HMK	01	0018	00	0	02	04	02
041100FF	DEP_ERAS6	01	0048	06	0	00	01	01
04130000	DEP_DES3	01	0018	00	1	05	00	01
04130100	DEP_DES1	01	0008	00	0	02	02	01
04130308	DEP_ERAS1	01	0008	00	0	00	01	01
04130500	DEP_DES2	01	0010	00	0	02	03	01
0425010A	DEP_M6	01	0018	06	0	00	01	01

5.4. TOOLBAR MENU

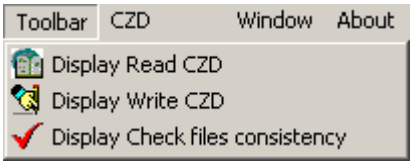
The **Toolbar** menu allows to hide or to display the shortcut buttons in the toolbar: *Read CZD*, *Write CZD* and *Check files consistency*.



By clicking on these menu items, the corresponding buttons disappear from the toolbar.

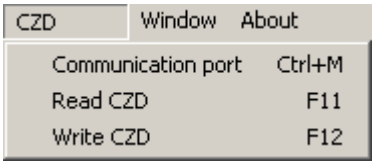


To make the toolbar buttons again visible, click once more on the menu items. Notice that their label was adapted to the context (*Hide* became *Display*).



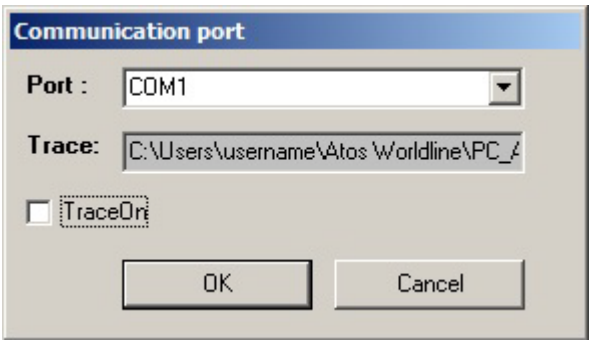
5.5. CZD MENU

The **CZD** menu allows defining the communication port, reading the *C-ZAM/DEP*'s Definition List files and writing Definition List files to the *C-ZAM/DEP*.



5.5.1. Communication port

Before working with the *C-ZAM/DEP*, verify that it is connected with the PC using the dedicated serial cable (see paragraph 4.1 on page 3). To select the correct communication port, select the **Communication port** menu item.



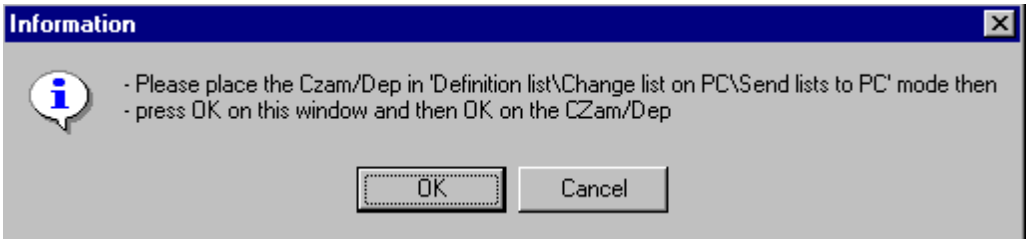
Make sure that the selected port is the good one because no hardware verification is done at this moment on the *C-ZAM/DEP*. It means that by pressing the *OK* button after having chosen the communication port, you only determine which port will be further used, during a **Read CZD** or a **Write CZD** operation.

If you click the *Cancel* button no communication port will be selected.
To log the messages select the *TraceOn* checkbox. The messages will be logged in the C:\Users\USERNAME\Atos Worldline\PC_AUX\Czd_trace.txt file. This can be useful to solve the communication problems.

5.5.2. Read CZD

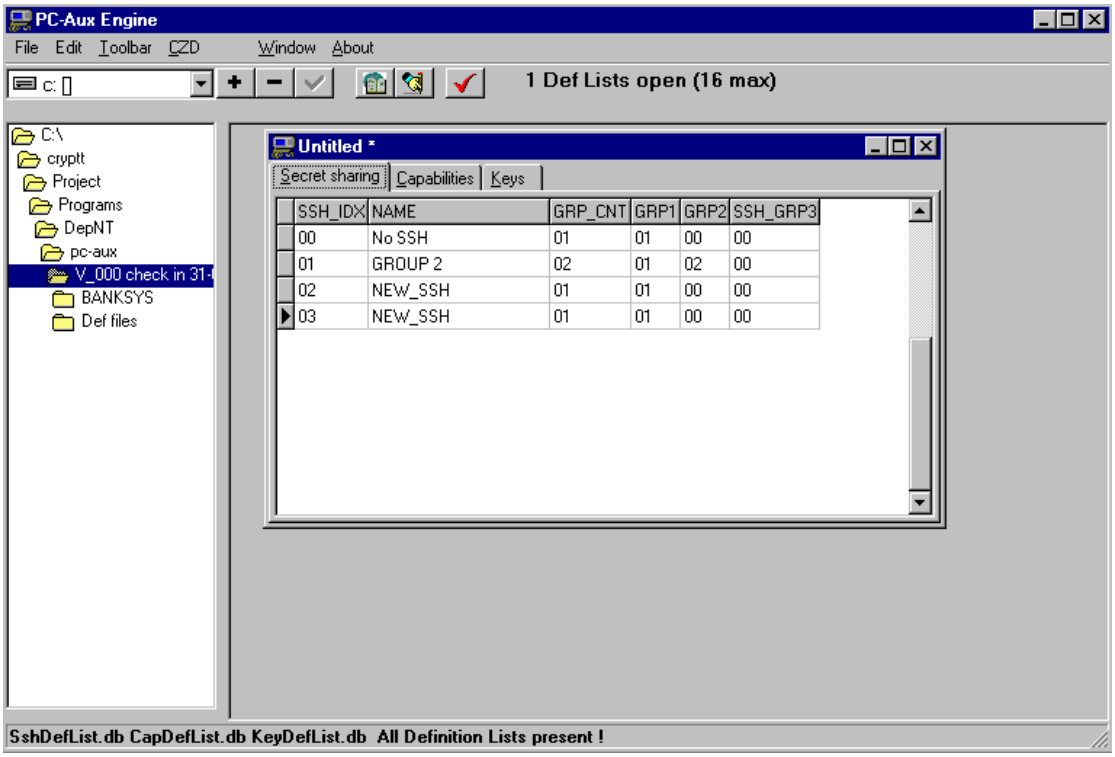
The **Read CZD** functionality is used to import the Definition List files already available in a *C-ZAM/DEP*. Refer to the *DEP C-ZAM/DEP User Manual* document for more information about getting Definition Lists in the memory of the *C-ZAM/DEP*.

First, verify that the C-ZAM/DEP is connected to the PC and the correct communication port is defined (see paragraph 5.5.1 on page 32), bring the C-ZAM/DEP in the correct mode to be able to send the Definition Lists (see *DEP C-ZAM/DEP User Manual* for this purpose) and select the **Read CZD** menu item.



Place the C-ZAMP/DEP in the indicated mode, confirm with *OK* in the application's information message and press the *C-ZAM/DEP*'s button *OK*. The Definition List will then be transferred from the *C-ZAM/DEP* to the PC.

After a successful transfer, a new sub-window appears.



Notice that the new sub-window has no title as the Definition List files are not yet saved in a folder. To save them, see paragraph 5.2.6 on page 21.

The Definition List can be read from the *C-ZAM/DEP* several times, as long as the limit of 16 sub-windows is not reached.

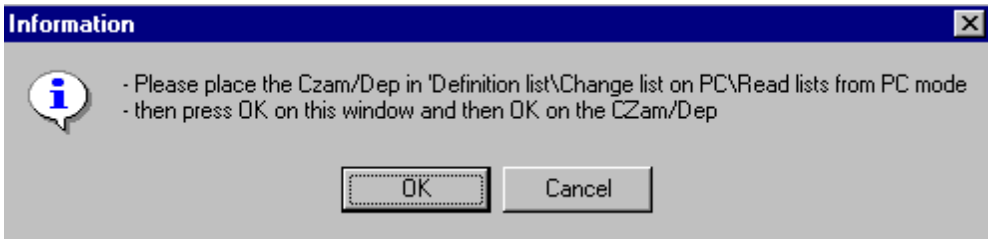
If the connection between the *C-ZAM/DEP* and the PC fails, an information message is received indicating how to solve the problem.

Remark that this functionality can also be launched by clicking on the  button in the toolbar.

5.5.3. Write CZD

The **Write CZD** functionality is used to transfer Definition List files from the PC to a *C-ZAM/DEP*. Typically, this function is used to modify the Definition Lists available in the *C-ZAM/DEP*.

First, verify that the *C-ZAM/DEP* is connected to the PC and the correct communication port is defined (see paragraph 5.5.1 on page 32), bring the *C-ZAM/DEP* in the correct mode to be able to receive the Definition Lists (see *DEP C-ZAM/DEP User Manual* for this purpose) and select the **Write CZD** menu item.



Place the C-ZAMP/DEP in the indicated mode, confirm with OK in the application's information message and press the *C-ZAM/DEP*'s OK button. The Definition List will then be transferred from the PC to the *C-ZAM/DEP*.

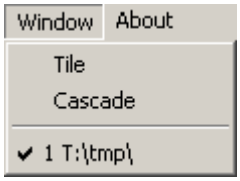
After a successful transfer, an information window appears.

Click OK to confirm. The Definition Lists are now available in the memory of the *C-ZAM/DEP*.

Remark that this functionality can also be launched by clicking on the  button in the toolbar.

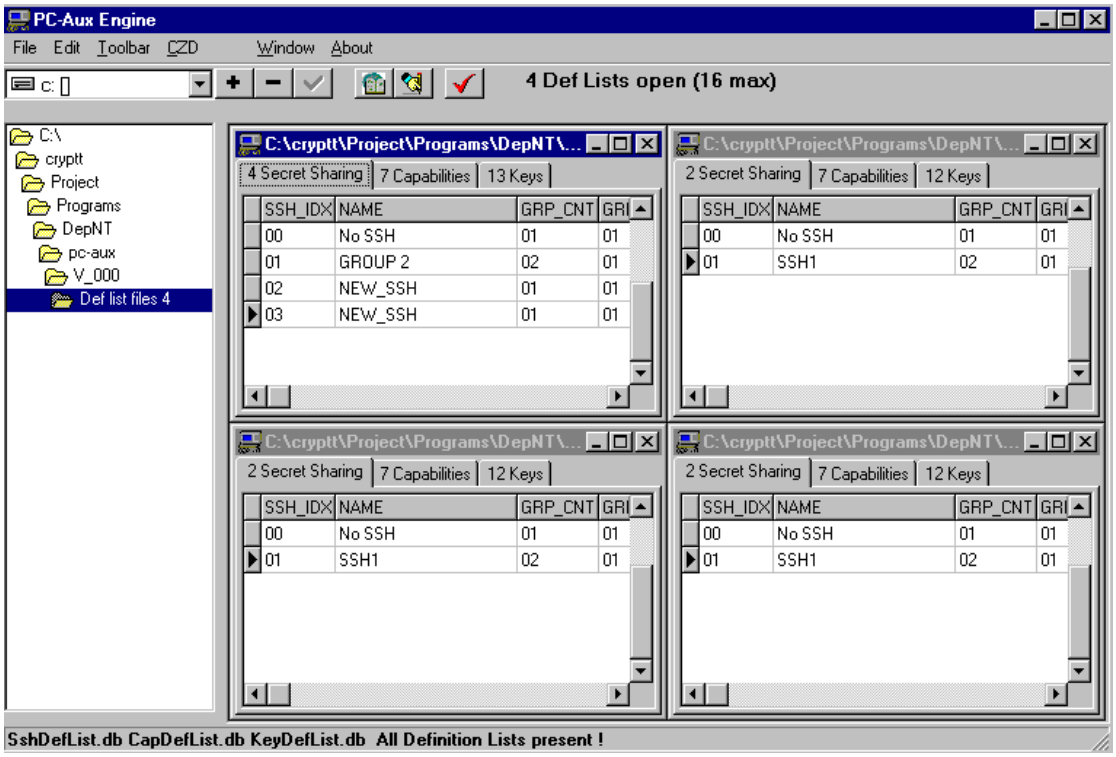
5.6. WINDOW MENU

The **Window** menu allows arranging the Definition List files' sub-windows following the **Tile** or the **Cascade** position. You can also set the **focus** on a determined sub-window by choosing it in the list constructed in the menu.



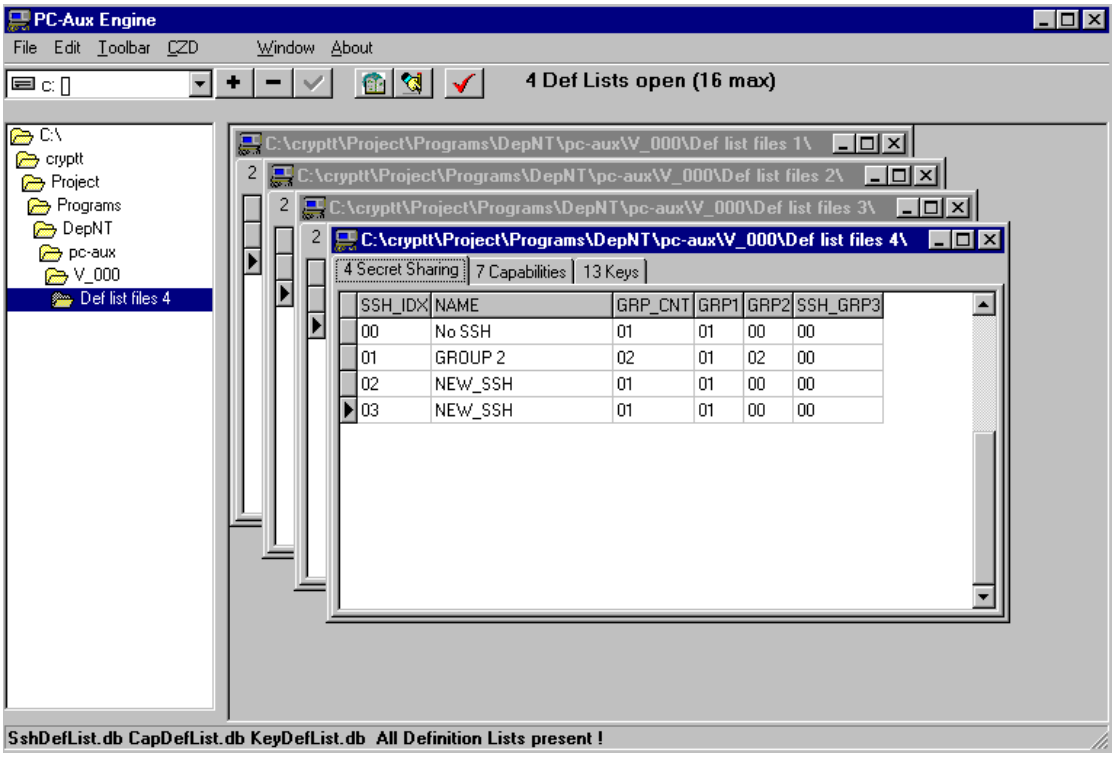
5.6.1. Tile

Click on the **Tile** menu item to arrange the sub-windows in the tile position.



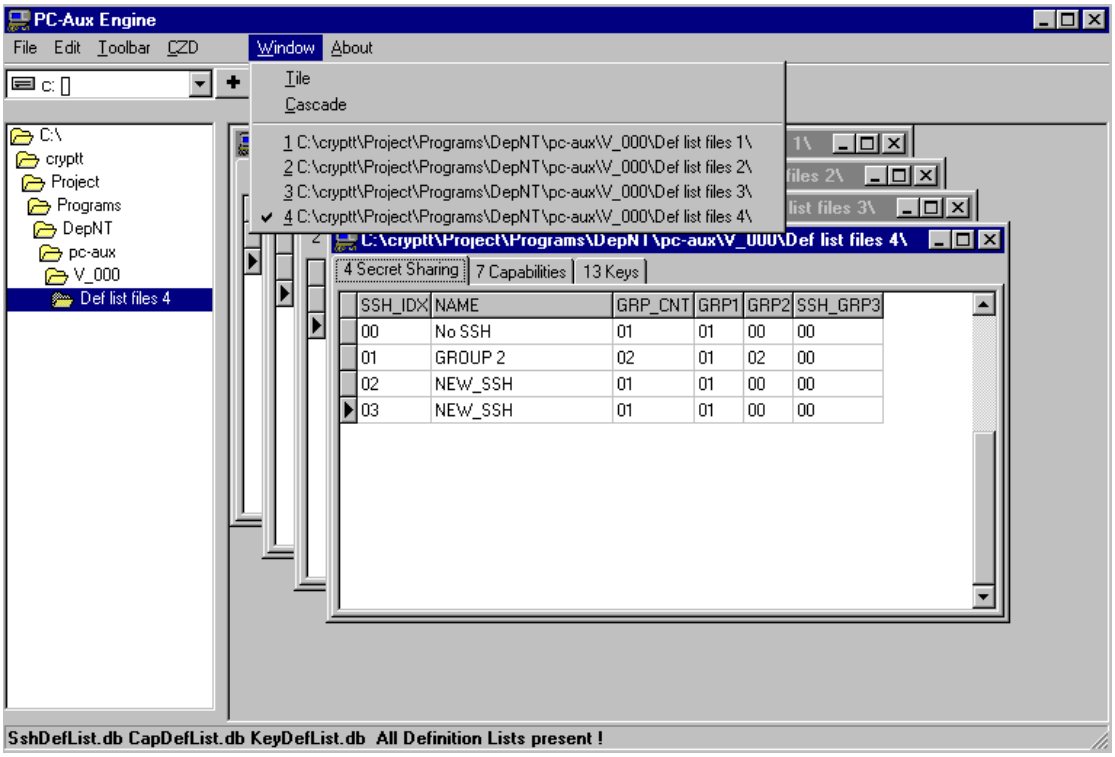
5.6.2. Cascade

Click on the **Cascade** menu item to arrange the sub-windows in the cascade position.



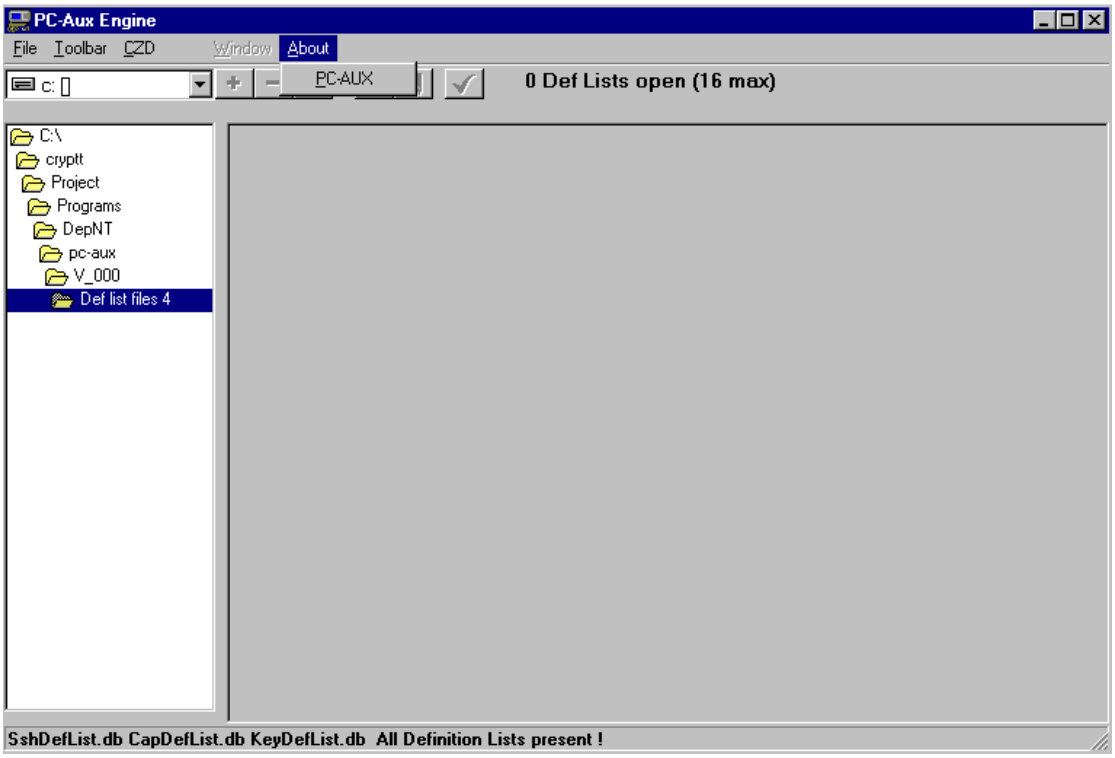
5.6.3. Focus

Focus on a determined window by choosing it in the list constructed in the menu. Focusing a sub-window means that it becomes active.



5.7. ABOUT MENU

The **About** menu gives information about the *DEP PC-AUX Program*.



Click on the **PC-AUX** menu item in the **About** menu to obtain information about the product.

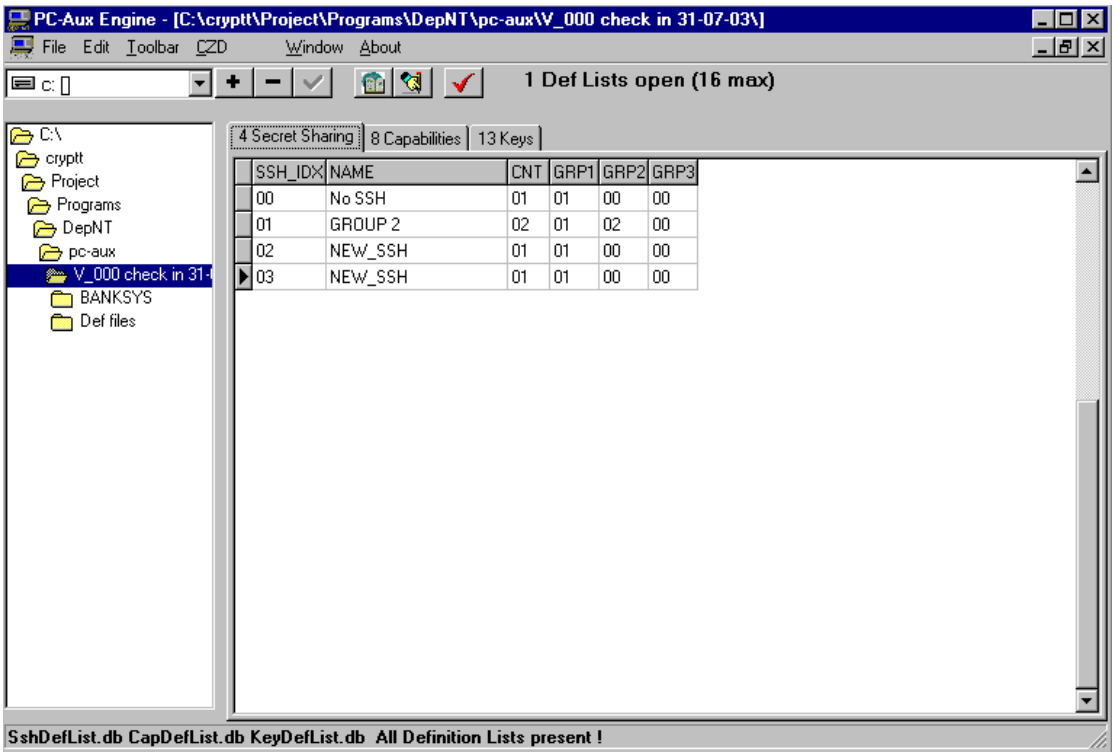
6. DEFINITION LISTS

Once the Definition Lists have been loaded into the *DEP PC-AUX Program*, they can be edited.

6.1. SECRET SHARING DEFINITION LIST

The Secret Sharing Definition List contains the properties of the Secret Sharing Schemes which are referenced to by the Key Definition List and the Capability Definition List. For more information about how secret sharing works, refer to *DEP Secret Sharing Mechanism* document.

To know which secret sharing definitions are needed for specific keys or specific capabilities, refer to the *DEP Atos Worldline' Security Officer's Guide* or to the *DEP Customer's Security Officer's Guide*.



A Secret Sharing Definition List can contain up to 30 records, but minimum one record is required in the *Secret Sharing*, *Capabilities* and *Keys* tabs.

Secret Sharing Definition List contains the following fields:

- **SSH_IDX** (1 byte): index identifying the secret sharing record (hexadecimal value from 00 to 1D)

- **NAME** (14 bytes): name (ASCII printable characters) describing the secret sharing record

- **CNT** (1 byte): number of secret sharing groups (value from 01 to 03)

- **GRP1** (1 byte): number of parts required in group 'one' to reconstruct the secret (value from 01 to 05)

- **GRP2** (1 byte): number of parts required in group 'two' to reconstruct the secret (value from 00 to 05)

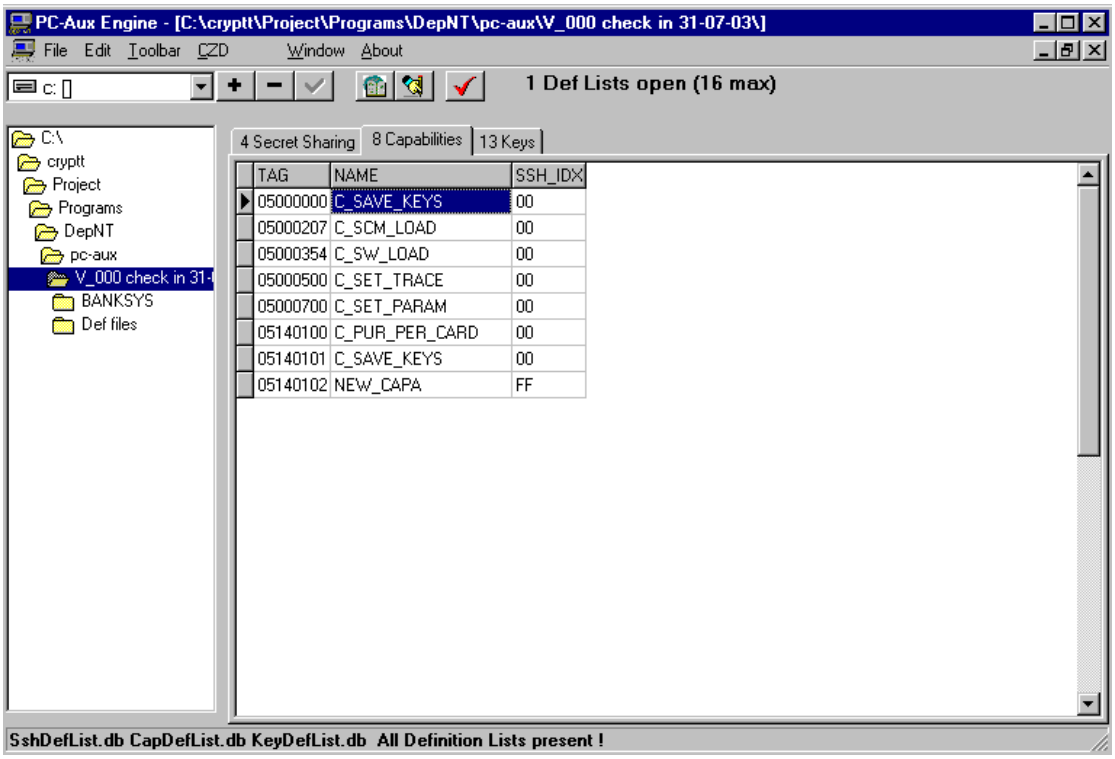
- **GRP3** (1 byte): number of parts required in group 'three' to reconstruct the secret (value from 00 to 05)

Every record must have a unique **SSH_IDX**.

The groups *GRPx* are completed in sequential order, i.e. when the *GRP3* is different from 00, then the *GRP2* must also be different from one. At least, the group *GRP1* must be defined.

6.2. CAPABILITY DEFINITION LIST

The Capability Definition List contains the properties of the DEP capabilities. To know which capabilities with which properties are required by the DEP environment or by a specific DEP software, refer to the *DEP Atos Worldline' Security Officer's Guide*, *DEP Customer's Security Officer's Guide* or to the dedicated software specification.



The Capabilities Definition List can contain up to 30 records, but minimum one record is required.

For each record, the following fields need to be entered:

- **TAG** (4 bytes): identification tag of the capability (value 05000000 to 05FFFFFF)
- **NAME** (14 bytes): name (ASCII printable characters) describing the capability record; this name appears also on the *C-ZAM/DEP*'s display
- **SSH_IDX** (1 byte): identifies the Secret Sharing Scheme linked to the capability; refers to the secret sharing index in the Secret Sharing Definition List (00 to 1D, FF)

Every record must have a unique *TAG*.

The *SSH_IDX* must be defined in the Secret Sharing Definition List. The value FF can be used when no Secret Sharing Scheme is associated to the capability (and thus cannot be saved on DCC).

6.3. KEY DEFINITION LIST

The Key Definition List contains the properties of DEP keys. To know which keys with which properties are required by the DEP environment or by a specific DEP software, refer to the *DEP Atos Worldline' Security Officer's Guide, DEP Customer's Security Officer's Guide* or to the dedicated software documentation.

The Keys Definition List can contain up to 600 records and minimum one record is required.

6.3.1. Novelty since version 3.0

Since the version 1.2.05, the *C-ZAM/DEP* has undergone several modifications concerning the check values mechanism. In order to support this new mechanism, the *DEP PC-AUX Program* (from version 3.0) was adapted and works now with new Key Definition Lists allowing the choice between several algorithms for the three check values of each key definition.

Fortunately, the old Key Definition Lists are always supported in the new *C-ZAM/DEP* and *DEP PC-AUX Programs*. However, the *DEP PC-AUX Program* gives the possibility to convert the old Key Definition List format into a new Key Definition List format (see paragraph 5.2.10 on page 24) and oppositely (see paragraph 5.2.9 on page 23).

6.3.2. Novelty since version 4.0

Since DEP PC-AUX Program version 4.0.1, it is possible to define 2 new features:

- AES key type
- Key Reconstruction method

These features have been merged into the new Definition List format, and the old format is still supported. Conversion between formats is also still supported. However, some data loss will occur while converting from new format to the old one. See paragraphs 5.2.10 and 5.2.9 on page 23. Following paragraphs concern the new and the old Key Definition Lists format working with the *PC-AUX program* since version 4.0.1.

6.3.3. Key Definition List fields

Key Definition Lists contain the following fields:

- **TAG** (4 bytes): identification tag of the key (value 04000000 to 04FFFFFF);
- **NAME** (14 bytes): name (ASCII printable characters) describing the key record; this name appears also on the *C-ZAM/DEP*'s display;
- **TYPE** (1 byte): identifies the type of the key;
- **LENGTH** (2 bytes): hexadecimal value representing the length of the key in bytes.
- **SSH_IDX** (1 byte): identifies the Secret Sharing Scheme linked to the key; refers to the secret sharing index in the Secret Sharing Definition List (00 to 1D, FF)
- **KR** (1 byte): identifies if the keys are reconstructed in C-ZAM/DEP or in DEP
- **ENTRY** (1 byte): identifies the key reconstruction method;
- **CV1, CV2, CV3** (1 byte): each field identifies a check value level and defines the algorithm for the calculation of this check value (the *DEP Key Entry Guide* gives a complete description of the check values' algorithms)
- **NO** (2 bytes): identifies the key in the key-table of a former generation of *Atos Worldline*' HSM (0000 to FFFF) or represents the last byte of the transport that will decrypt the values loaded in the *C-ZAM/DEP* depending on the ENTRY field.

Every record must have a unique key *TAG*. Besides, the *SSH_IDX* must be defined in the Secret Sharing Definition List. The value FF can be used when no secret sharing scheme is associated to the key (and thus cannot be saved on DCC).

6.3.4. Common fields for old/new Key Definition Lists

The fields **TAG**, **NAME**, **TYPE**, **LENGHT** and **SSH_IDX** are common for both the old and the new Key Definition Lists.

6.3.5. Specific values for old Key Definition List

Some fields are specific for the old Key Definition List.

- **TYPE** (1 byte): identifies if the key is DES or RSA
  → **01** (DES key)
  → **02** (RSA key)

- **LENGTH** (2 bytes): hexadecimal value representing the length of the key in bytes
  - For DES key, proposed values are:
  0008 (DES1), **0010** (DES2), **0018** (DES3)
  - For RSA keys, proposed values are:
  0040 (RSA 512 bits), **0080** (RSA 1024 bits)

- **ENTRY**[1] (1 byte): identifies how the key values can be created in the *C-ZAM/DEP* and which check value algorithm is applied
  → **00** (RAND): keys are generated randomly by the *C-ZAM/DEP* (DES keys only)
  → **01** (DS2): keys come from a *DS2* key backup file
  → **02** (FULL): manual key loading per block of eight bytes, every block has a *FULL* check value
  → **03** (NORM): manual key loading per block of eight bytes, every block has a *NORM* check value
  → **04** (NONE): manual key loading per block of eight bytes, without any check value
  → **05** (POOL): manual key loading according to the *POOL* definition
  → **06** (ENC): manual loading per block of eight bytes, every block entered is decrypted with another key (*K_AB*); the loading of this decrypted key must be followed by a check value defined as the six leftmost bytes of the encrypted value $E_{clear\_key}(00000000)$
  → **07** (XOR2): manual loading per block of eight bytes and each part is divided in two sub-parts XORed; each of the sub-parts have a check value *NORM*
  → **08** (XOR3): manual loading per block of eight bytes and each part is divided in three sub-parts XORed; each of the sub-parts have a check value *NORM*

[1] This field was formerly called *KEY_GEN*.

→ **09** (XR2A): manual loading per block of eight bytes and each part is divided in two sub-parts XORed; the first sub-part has a check value *NORM*, the last has a check value *NORM* over the XORed key
→ **0A** (XR3A): manual loading per block of eight bytes and each part is divided in three sub-parts XORed; the two first sub-part have a check value *NORM*, the last has a check value *NORM* over the XORed key
→ **0B** (DX3): manual loading associating a XOR3 with the introduction of a block of eight bytes. The last block is decrypted with the XORed key and a check value NORM is computed on the result of the decrypted key.

- **CV1** (1 byte), **CV2** (1 byte), **CV3** (1 byte): are not used in case of old Key Definition Lists (see paragraph 6.4.1 on page **Error! Bookmark not defined.**).

- **NO** (2 bytes)
  → when the *ENTRY* field equals "01 (DS2)", the field's value is the identification of the key in the key-table of a former generation of *Atos Worldline*' HSM (0000 to FFFF); in this case, the column's name changes into "SLOT"
  → when the *ENTRY* field has another value, the field is not used (read-only and the value is set to "0000")

More information about the way the keys are entered (different entry modes) can be found in the document *DEP Key Entry Guide*.

6.3.6. Specific values for new Key Definition List

Some fields are specific for the new Key Definition List.

- **TYPE** (1 byte): identifies the type of the key
  → **01** (DES key)
  → **02** (RSA key)
  → **04** (AES key)

- **LENGTH** (2 bytes): hexadecimal value representing the length of the key in bytes
  - For DES key, proposed values are:
  0008 (DES1), **0010** (DES2), **0018** (DES3)
  (other values – up to DES10 – can be introduced manually)

  - For RSA keys, proposed values are:
  0040 (RSA 512 bits), **0080** (RSA 1024 bits)

  - For AES key, proposed values are:
  0010 (AES 128 bits), **0018** (AES 192 bits), **0020** (AES 256 bits)

- **KR** (1 byte): identifies where the keys are reconstructed

→ **00** (CZD): key is reconstructed in the CZAM/DEP
→ **01** (DEP): key is reconstructed in the DEP

- **ENTRY** (1 byte):
  - For keys reconstructed in the CZAM/DEP, the proposed values are:
    → **00** (RAND): keys are generated randomly by the *C-ZAM/DEP* (DES keys only); there is no check value for this type
    → **01** (DS2): keys come from a *DS2* key backup file; there is no check value for this type
    → **02** (DEF): manual key loading of clear text key per block of eight bytes
    → **03** (POOL): manual key loading according to the *POOL* definition
    → **04** (ENC): manual loading of an encrypted key per block of eight bytes, every block entered is decrypted with a single DES transport key (*K_AB*)
    → **05** (XOR2): manual loading per block of eight bytes and each part is divided in two sub-parts XORed
    → **06** (XOR3): manual loading per block of eight bytes and each part is divided in three sub-parts XORed
    → **07** (XR2A): manual loading per block of eight bytes and each part is divided in two sub-parts XORed (same as XOR2)
    → **08** (XR3A): manual loading per block of eight bytes and each part is divided in three sub-parts XORed (same as XOR3)
    → **09** (DX3): manual loading of an encrypted key per block of eight bytes; the single DES transport key is introduced as an XOR3 and every block entered is decrypted with a single DES XORed transport key
    → **0A** (ENC2): manual loading of an encrypted key per block of eight bytes; every block entered is decrypted by an external transport key (single, double or triple DES key); at least one transport key must have been previously defined in the Key Definition List (the tag of a transport key always begins with "04F0F0" + one byte ("00" to "FF") representing the key instance (these key instances is filled in the field *INST* of the *ENC2* keys and will point on their related transport key)

  - For keys reconstructed in the DEP, the proposed values are:
    → **05** (XOR2): manual loading per block of eight bytes and each part is divided in two sub-parts XORed
    → **06** (XOR3): manual loading per block of eight bytes and each part is divided in three sub-parts XORed
    → **0A** (ENC2): manual loading of an encrypted key per block of eight bytes; every block entered is decrypted by an external transport key (single, double or triple DES key); at least one transport key must have been previously defined in the Key Definition List (the tag of a transport key always begins with "04F0F0" + one byte ("00" to "FF") representing the key instance (these key instances is filled in the field *INST* of the *ENC2* keys and will point on their related transport key)
    → **0B** (SSH): manual loading per block of eight bytes and each part is

divided in a certain number of sub-parts, reconstructed using *Secret Sharing* scheme. The scheme used (number of groups, number of parts per group) is determined by the value of the SSH_IDX.

- **CV1, CV2, CV3** (1 byte): each field identifies a check value level and defines the algorithm for the calculation of this check value (the *DEP Key Entry Guide* gives a complete description of the check values' algorithms)
  - If the value of ENTRY is 00 (RAND), all CV's are always 01 (NORM)

  - For keys reconstructed in the CZAM/DEP, the proposed values are:
    → **01** (NONE): no check value will be applied on key introduced.
    → **02** (NORM): check value based on the encryption of a null data by a key E_{key}("0000000000000000").
    → **03** (FULL): check value based on the encryption of a key by the key itself E_{key}(key).
    → **04** (ISO10118-2): check value based on the calculation of a hash value

  - For keys reconstructed in the DEP, the value of *CV1* is always 00 (NONE), for *CV2* and *CV3*, the proposed values are:
    → **01** (NONE): no check value will be applied on key introduced.
    → **02** (NORM): check value based on the encryption of a null data by a key E_{key}("0000000000000000").
    → **04** (ISO10118-2): check value based on the calculation of a hash value

- **NO** (2 bytes): three cases must be considered:
  → when the *ENTRY* field equals "01 (DS2)", the field's value is the identification of the key in the key-table of a former generation of *Atos Worldline*' HSM (0000 to FFFF); in this case, the column's name changes into "*SLOT*" and is coded on four digits
  → when the *ENTRY* field equals "0A (ENC2)", the field's value (coded on two digits) represents the last byte of the transport that will decrypt the values loaded in the *C-ZAM/DEP*; in this case, the column's name changes into "*INST*"
  → when the *ENTRY* field has another value, the field is not used (read-only and the value is set to "0000")

More information about the way the keys are entered (different entry modes) can be found in the document *DEP Key Entry Guide*.

6.3.7. Field dependency table

For clarity, here are two tables that show the dependency between the fields of new Key Definition List, and proposed values in each case.

TYPE	LENGTH
01 DES	0008 DES1

	0010 DES2 0018 DES3
02 RSA	0040 RSA (512 bits) 0080 RSA (1024 bits)
04 AES	0010 AES (128 bits) 0018 AES (192 bits) 0020 AES (256 bits)

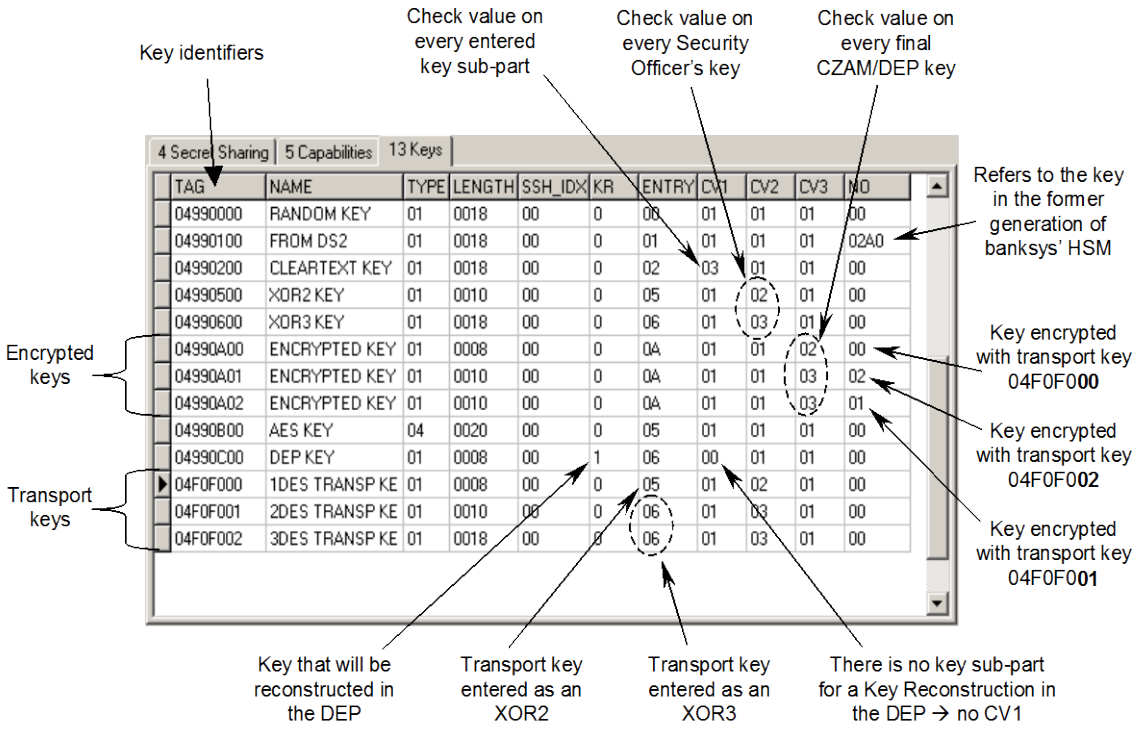
KR	ENTRY	CV1	CV2	CV3
0 CZD	00 RAND	01 NORM		
	01 DS2 02 DEF 03 POOL 04 ENC 05 XOR2 06 XOR3 07 XR2A 08 XR3A 09 DX3 0A ENC2	00 NONE 01 NORM 02 FULL 03 ISO 10118-2		
1 DEP	05 XOR2 06 XOR3 0A ENC2	01 NONE	02 NONE 03 NORM[2] 03 ISO 10118-2	

6.3.8. Example

An example of Key Definition List, which is encoded in the new Definition List format, is shown in this paragraph. It lists the most used key entry modes and explains the most important properties. See also the document *DEP Key Entry Guide* for more information.

Remark that for the check value levels, the advice is followed as described in the *DEP Key Entry Guide*.

[2] For DES4 up to DES10 keys, NORM is not supported.



TAG	NAME	TYPE	LENGTH	SSH_IDX	KR	ENTRY	CV1	CV2	CV3	MD
04990000	RANDOM KEY	01	0018	00	0	00	01	01	01	00
04990100	FROM DS2	01	0018	00	0	01	01	01	01	02A0
04990200	CLEARTEXT KEY	01	0018	00	0	02	03	01	01	00
04990500	XOR2 KEY	01	0010	00	0	05	01	02	01	00
04990600	XOR3 KEY	01	0018	00	0	06	01	03	01	00
04990A00	ENCRYPTED KEY	01	0008	00	0	0A	01	01	02	00
04990A01	ENCRYPTED KEY	01	0010	00	0	0A	01	01	03	02
04990A02	ENCRYPTED KEY	01	0010	00	0	0A	01	01	03	01
04990B00	AES KEY	04	0020	00	0	05	01	01	01	00
04990C00	DEP KEY	01	0008	00	1	06	00	01	01	00
04F0F000	1DES TRANSP KE	01	0008	00	0	05	01	02	01	00
04F0F001	2DES TRANSP KE	01	0010	00	0	06	01	03	01	00
04F0F002	3DES TRANSP KE	01	0018	00	0	06	01	03	01	00